

საქართველოს განათლებისა და მეცნიერების სამინისტრო
შიდა ქართლის საერო უნივერსიტეტი

ციური ნოზაძე, ზურაბ თეთრუაშვილი, სოსო ნოზაძე

კომპიუტერული ქსელები
ინტერნეტი
კომპიუტერული უსაფრთხოება

თბილისი
2007

თანამედროვე მსოფლიოში სავაჭრო თუ საწარმოო ურთიერთობებში ჩაბმულია უამრავი კერძო თუ სახელმწიფო სუბიექტი. ქვეყნებს შორის ეკონომიკური ურთიერთობების გაღრმავების სულ უფრო მზარდი მოთხოვნების დაკმაყოფილება შეუძლებელია შესაბამისი საკომუნიკაციო მომსახურების გარეშე.

თანამედროვე საკომუნიკაციო საშუალებებიდან ყველაზე პოპულარული სამსახური – ინტერნეტი, დღეისათვის ნებისმიერ კონტინენტზე არა მარტო ადამიანების პირადი კომუნიკაციის საშუალებაა, არამედ ფირმების ეკონომიკური ურთიერთობების განხორციელების სწრაფი და მოქნილი საშუალებაც.

წიგნში განხილულია თანამედროვე კომუნიკაციის საშუალებების აგებისა და გამოყენების საკითხები. იგი განკუთვნილია მათთვის, ვინც გადაწყვიტა დამოუკიდებლად ჩაწვდეს თანამედროვე საკომუნიკაციო საშუალებების არსსა და სამსახურებს, ინტერნეტის მუშაობის ზოგად პრინციპებსა და პროგრამულ უზრუნველყოფას.

მკითხველს ვთხოვთ შენიშვნები და მოსაზრებები გამოავზაენოთ მისამართზე: გორი 1400, საქართველო, ცხინვალის გზატკეცილი 9/2, შიდა ქართლის საერო უნივერსიტეტი.

E-mail: university@sknu.edu.ge
znozadze@rambler.ru

რედაქტორი: გიორგი უბირია, ბარ-ილანის უნივერსიტეტის
დოქტორი;

ბაჟინჟარი რედაქტორი: ილია მურადელი.

წიგნი იბეჭდება შიდა ქართლის საერო უნივერსიტეტის სამეცნიერო საბჭოს გადაწყვეტილებით და ამავე უნივერსიტეტის ფინანსური მხარდაჭერით.

ISBN 978-99940-68-68-5

შინაარსი

თავი 1. კომპიუტერული ქსელები, ინტერნეტი.....	5
1.1 კომპიუტერული ქსელების არსი და მნიშვნელობა.....	5
1.2 ლოკალური და გლობალური ქსელები.....	7
1.3 ინტერნეტის განვითარების ისტორია.....	10
1.4 ინტერნეტის ძირითადი ცნებები.....	13
1.5 ინტერნეტის სამსახურები.....	17
1.6 ინტერნეტთან შეერთება.....	33
თავი 2. ინფორმაციის მიღება ინტერნეტიდან.....	38
2.1 World Wide Web – ძირითადი ცნებები.....	38
2.2 Internet Explorer პროგრამასთან მუშაობა.....	42
2.3 Web გვერდის დათვალიერება.....	44
2.4 ბრაუზერის მართვის მეთოდები.....	46
2.5 ფაილების მიღება ინტერნეტიდან.....	52
2.6 ინფორმაციის ძებნა ინტერნეტში.....	54
2.7 თანამედროვე საძიებო მიმთითებლების ძირითადი პრობლემები.....	64
2.8 უახლესი საძიებო ტექნოლოგიები.....	66
2.9 ეფექტური ძებნის ხერხები.....	70
2.10 საძიებო სისტემების გამოყენების რეკომენდაციები.....	71
თავი 3. ელექტრონული ფოსტა.....	74
3.1 ზოგადი მიმოხილვა.....	74
3.2 ელექტრონულ ფოსტასთან მუშაობის ზოგადი წესები.....	76
3.3 WWW-ზე დაფუძნებული ელექტრონული ფოსტა.....	78

3.4	ელექტრონული ფოსტის შეტყობინებების სტრუქტურა.....	81
3.5	საფოსტო კლიენტების ფუნქციები და თვისებები.....	82
3.6	საფოსტო კლიენტების დამატებითი ფუნქციები.....	86
3.7	ელექტრონული ფოსტის საშუალებების სპეციალური ფუნქციები.....	94
3.8	ელექტრონული ფოსტის ეთიკა.....	98
3.9	ელექტრონული ფოსტის უსაფრთხოება.....	104

თავი 4. კომპიუტერული უსაფრთხოება..... 108

4.1	კომპიუტერული უსაფრთხოების ცნება.....	108
4.2	კომპიუტერული ვირუსებისაგან დაცვის მეთოდები.....	112
4.3	ინფორმაციის დაცვა ინტერნეტ ში.....	116
4.4	ინფორმაციული უსაფრთხოება.....	118
4.5	ქსელური უსაფრთხოების რეჟიმის დარღვევის ძირითადი სახეები.....	123
4.6	ინტერნეტის ზოგიერთი სასარგებლო გვერდები.....	140

თავი 1. კომპიუტერული ქსელები, ინტერნეტი

1.1 კომპიუტერული ქსელების არსი და მნიშვნელობა.

კომპიუტერული ქსელი ორი ან მეტი კომპიუტერის ფიზიკური შეერთებით წარმოიქმნება. საერთოდ, კომპიუტერული ქსელების შესაქმნელად აუცილებელია სპეციალური აპარატული (ქსელის მოწყობილობები) და სპეციალური პროგრამული (*ქსელის პროგრამები*) საშუალებები. ორი კომპიუტერის უმარტივეს შეერთებას მონაცემების გაცვლისათვის პირდაპირი შეერთება ეწოდება. კომპიუტერების პირდაპირი შეერთების შესაქმნელად, რომლებიც Windows ოპერაციულ სისტემაში მუშაობენ, საჭირო არაა სპეციალური აპარატული და პროგრამული საშუალებები. ამ შემთხვევაში აპარატულ საშუალებებს წარმოადგენენ შეტანა-გამოტანის სტანდარტული პორტები (მიმდევრობითი ან პარალელური), ხოლო პროგრამული უზრუნველყოფის სახით გამოიყენება ოპერაციული სისტემის სტანდარტული საშუალებები. [Start ▶ Programm ▶ Accesories ▶ Communications ▶ Network Connections].

განურჩევლად ყველა კომპიუტერულ ქსელებს აქვთ ერთი დანიშნულება - საერთო რესურსებთან ერთობლივი შეღწევის უზრუნველყოფა. სიტყვა *რესურსი* აქ მოხერხებულია რადგან ქსელის დანიშნულების მიხედვით მასში შეიძლება ჩავდეთ ესა თუ ის აზრი. რესურსები სამი ტიპისაა: *აპარატული, პროგრამული და ინფორმაციული*. მაგალითად, ბეჭდვის მოწყობილობა (პრინტერი) - აპარატული რესურსია. ხისტი დისკის (ვინჩესტერი) ტევადობა აგრეთვე აპარატული რესურსია. როდესაც მცირე კომპიუტერული ქსელის ყველა მომხმარებელი იყენებს ერთ

საერთო პრინტერს, მაშასადამე ისინი იყენებენ საერთო აპარატურულ რესურსს. იგივე შეიძლება ითქვას ქსელზე, რომელსაც აქვს გაზრდილი ტევადობის ხისტი დისკი (*ვარიანტის სერვერი*), რომელზეც ქსელის ყველა მომხმარებელი ინახავს თავის არქივებს და მუშაობის შედეგებს.

გარდა აპარატურული რესურსებისა, კომპიუტერული ქსელები იძლევიან *პროგრამული რესურსების* ერთობლივ გამოყენების საშუალებასაც. ასე მაგალითად, როული და ხანგრძლივი გამოთვლების შესასრულებლად შეიძლება დავუკავშირდეთ დაშორებულ, დიდ კომპიუტერს და გავაგზავნოთ მასზე გამოთვლების დავალება, ხოლო გამოთვლების დამთავრების შემდეგ ამავე გზით მივიღოთ შედეგები.

მონაცემები, რომლებიც ინახება დაშორებულ კომპიუტერზე ქმნიან ინფორმაციულ რესურსს. ამ რესურსების როლი ნათლად ჩანს ინტერნეტის მაგალითზე, რომელიც აღიქმება როგორც გიგანტური ინფორმაციულ-საცნობარო სისტემა.

რესურსების აპარატურულ, პროგრამულ და ინფორმაციულ რესურსებად დაყოფის ეს მაგალითები საკმაოდ პირობითია. სინამდვილეში, ნებისმიერი ტიპის კომპიუტერულ ქსელში მუშაობისას ხდება ყველა ტიპის რესურსების ერთობლივი გამოყენება. ასე მაგალითად, მივმართავთ რა ინტერნეტს ცნობებისათვის სადამოს ტელეგადაცემების შესახებ, ჩვენ აუცილებლად ვიყენებთ აპარატურულ საშუალებას, რომლებშიც მუშაობენ ვიდაცის პროგრამები, რომლებიც უზრუნველყოფენ მოთხოვნილი მონაცემების მოწოდებას.

1.2 ლოკალური და გლობალური ქსელები.

კომპიუტერულ ქსელებში, როგორც აპარატურის, ასევე პროგრამების თავსებადობის უზრუნველსაყოფად მოქმედებს სპეციალური სტანდარტები, რომლებსაც *პროტოკოლებს* უწოდებენ. პროტოკოლები განსაზღვრავენ, როგორც ქსელის აპარატული კომპონენტების ურთიერთქმედების ხასიათს და მათ *აპარატული პროტოკოლებს* უწოდებენ, ასევე პროგრამების და მონაცემების ურთიერთქმედების ხასიათს, რომლებსაც *პროგრამულ პროტოკოლებს* უწოდებენ. ფიზიკურად პროტოკოლების დაცვის ფუნქციებს ასრულებენ აპარატული მოწყობილობები (*ინტერფეისი*) და პროგრამული საშუალებები (*პროტოკოლის მომსახურების პროგრამები*). პროგრამებს, რომლებიც უზრუნველყოფენ პროტოკოლის მომსახურებას ხშირად პროტოკოლებსაც უწოდებენ.

ასე მაგალითად, თუ ორი კომპიუტერი ერთმანეთთან პირდაპირი შეერთებითაა დაკავშირებულია, მაშინ ფიზიკურ დონეზე მათი ურთიერთქმედების პროტოკოლს განსაზღვრავენ ფიზიკური პორტის (პარალელური ან მიმდევრობითი) კონკრეტული მოწყობილობები და მექანიკური კომპონენტები (ჩამრთველები, კაბელი და სხვა). უფრო მაღალ დონეზე კომპიუტერების ურთიერთქმედებას განსაზღვრავენ მონაცემების გადაცემის მართვის პროგრამული საშუალებები. ყველაზე მაღალ დონეზე ურთიერთქმედების პროტოკოლს უზრუნველყოფენ ოპერაციული სისტემის დანართი პროგრამები. მაგალითად, Windows-ისათვის ესაა სტანდარტული პროგრამა-პირდაპირი საკაბელო შეერთება [Network Connections].

გამოყენებული პროტოკოლების შესაბამისად მიღებულია კომპიუტერული ქსელების დაყოფა ლოკალურ (*LAN-Local Area Network*) და გლობალურ (*WAN -Wide Area Network*) ქსელებად. ლოკალური ქსელის კომპიუტერები უმეტესად გამოიყენებენ პროტოკოლების ერთიან კომპლექტს ყველა მონაწილისათვის. ტერიტორიული ნიშნის მიხედვით ლოკალური ქსელები განსხვავდება კომპაქტურობით. ისინი შეიძლება აერთიანდნენ ერთი შენობის, სართულის, ოთახის, კომპაქტურად განლაგებული ნაგებობების კომპიუტერების ჯგუფს. გლობალურ ქსელებს, როგორც წესი აქვთ გაზრდილი გეოგრაფიული ზომები. მათ შეუძლიათ გააერთიანონ როგორც ცაკლეული კომპიუტერები, ასევე ცაკლეული ლოკალური ქსელები, მათ შორის ისეთებიც, რომლებიც სხვადასხვა პროტოკოლებს იყენებენ.

თანამშრომელთა ჯგუფს, რომლებიც ლოკალური ქსელის ფარგლებში ერთ პროექტზე მუშაობენ *მუშა ჯგუფებს* უწოდებენ. ერთი ლოკალური ქსელის ფარგლებში შეიძლება მუშაობდეს რამოდენიმე მუშა ჯგუფი. მუშა ჯგუფის მონაწილეებს შეიძლება ქონდეთ ქსელის საერთო რესურსებით სარგებლობის სხვადასხვანაირი უფლება. კომპიუტერული ქსელის მონაწილეების უფლებების განაწილებისა და შეზღუდვის წესების ერთობლიობას *ქსელის პოლიტიკას* უწოდებენ. ქსელის პოლიტიკის (ის შეიძლება ოყოს რამოდენიმე ერთ ქსელში) მართვას ადმინისტრირებას უწოდებენ. პირს, რომელიც ლოკალური კომპიუტერული ქსელის მუშაობის ორგანიზაციას მართავს *სისტემურ ადმინისტრატორს* უწოდებენ.

ლოკალური ქსელების შექმნა დამახასიათებელია ცალკეული საწარმოებისა ან საწარმოების ცალკეული ქვე-

განყოფილებებისათვის. თუ საწარმოს (ან დარგს) უკავია დიდი ტერიტორია, მაშინ ცაკლეული ლოკალური ქსელები შეიძლება გაერთიანდნენ გლობალურ ქსელში. ასეთ შემთხვევაში ლოკალურ ქსელებს ერთმანეთს უკავშირებენ ნებისმიერი, ტრადიციული კავშირის არხებით (საკაბელო, თანამგზავრი, რადიოსარელო და სხვა). როგორც შემდეგში ვნახავთ ამ მიზნისათვის სპეციალური პირობების დაცვით შეიძლება გამოყენებული იქნას სატელეფონო არხები, თუმცა ისინი ყველაზე ნაკლებად აკმაყოფილებენ ციფრული კავშირის პირობებს.

სხვადასხვა პროტოკოლებით მომუშავე რამოდენიმე ლოკალური ქსელის ურთიერთკავშირს ემსახურება სპეციალური საშუალებები- *შლიუზები*. შლიუზები შეიძლება იყოს როგორც აპარატული, ასევე პროგრამული. მაგალითად, იგი შეიძლება იყოს სპეციალური კომპიუტერი (*შლიუზერული სერვერი*), ან კომპიუტერული პროგრამა - შლიუზერული დანართი. ბოლო შემთხვევაში კომპიუტერს შეუძლია შეასრულოს არა მარტო შლიუზერის ფუნქცია არამედ მუშა სადგურებისათვის დამახასიათებელი სხვა რომელიმე ტიპური ფუნქცია.

საწარმოს ლოკალური ქსელის გლობალურ ქსელთან მიერთებისას მნიშვნელოვანია *ქსელის უსაფრთხოების* დაცვა. კერძოდ, შეზღუდული უნდა იქნას ლოკალურ ქსელში გარედან უცხო პირების დაშვება, ასევე შეზღუდულია ლოკალური ქსელის ფარგლებს გარეთ გასვლა საწარმოს იმ თანამშრომლებისათვის, რომლებსაც არა აქვთ შესაბამისი უფლება. ქსელური უსაფრთხოების უზრუნველსაყოფად ლოკალურ და გლობალურ ქსელებს შორის აყენებენ ეგრეთწოდებულ *ბრანდმაუერებს*. ბრანდმაუერი შეიძლება იყოს სპეციალური კომპიუტერი ან

კომპიუტერული პროგრამა, რომელიც ეწინააღმდეგება ქსელებს შორის მონაცემების არასანქცირებულ გადაადგილებას.

1.3 ინტერნეტის განვითარების ისტორია.

კომპიუტერის საშუალებით ინფორმაციის მიღება-გადაცემის ადრეული ექსპერიმენტები დაიწყო ჯერ კიდევ *^* საუკუნის 50-ან წლებში და ლაბორატორიული ხასიათი ჰქონდა. ამერიკის შეერთებულ შტატებში პირველი ნაციონალური მასშტაბის გლობალური ქსელის შექმნის გადაწყვეტილება მიღებული იყო 1958 წელს, რომელიც გახლდათ რეაქცია ყოფილ საბჭოთა კავშირში დედამიწის პირველი ხელოვნური თანამგზავრის გაშვებაზე.

გლობალური კომპიუტერული ქსელის შექმნის საბაზი პენტაგონის მიერ რაკეტების გაშვების შესახებ ადრეული შეტყობინებების გლობალური სისტემის (*NORAD-North American Aerospace Defance Command*) დამუშავება გახდა. სისტემის სადგურები განლაგებული იყო კანადის ჩრდილოეთით ალიასკიდან გრენლანდიამდე, ხოლო მიწისქვეშა საბრძანებო პუნქტი ქალაქ კოლორადო-სპრინგის მახლობლად, მთა შეინის წიადში. მართვის ცენტრი მოქმედებაში შევიდა 1964 წელს და სწორედ ამ დროიდან დაედო სათავე პირველი გლობალური საუწყებო კომპიუტერული ქსელის მუშაობას. 60-იანი წლების შუა პერიოდიდან მას შეუერთდნენ საავიაციო, მეტეოროლოგიური და სხვა სამხედრო და სამოქალაქო სამსახურები.

ქსელის მუშაობას კურირებდა სპეციალური ორგანიზაცია, აშშ-ს თავდაცვის სამინისტროს პერსპექტიული დამუშავებების სამმართველო (*DARPA-Defense Advansed Research*

Project Agency). ცენტრალიზებული ქსელის ძირითადი ნაკლი იყო არასაკმარისი მდგრადობა, რომელიც დაკავშირებული იყო იმასთან, რომ რაიმე კვანძის მწყობრიდან გამოსვლისას, მწყობრიდან გამოდიოდა მისი მთელი მომდევნო სექტორი, ხოლო მართვის ცენტრის მწყობრიდან გამოსვლისას კი მთელი ქსელი. ზესახელმწიფოების ბირთვული დაპირისპირების ხანაში ეს ნაკლი მეტად კრიტიკული იყო.

ქსელის მდგრადობისა და საიმედოობის პრობლემების გადაწყვეტა დაევალა სამართველო *DARPA*. კვლევის ძირითადი მიმართულებები ქსელის მომსახურების ახალი პრინციპების ძიება გახდა. ახალი პრინციპების გამოცდის პოლიგონები გახდნენ აშშ-ის მსხვილი უნივერსიტეტები და სამეცნიერო ცენტრები, რომელთა შორის გაყვანილი იყო კომპიუტერული კავშირის ხაზები. თავდაცვის სამინისტროს მხრიდან სამუშაოებს კურირებდა იგივე სამართველო *DARPA* და პირველმა არასაუწყებო ნაციონალურმა კომპიუტერულმა ქსელმა, რომელიც 1969 წელს დაინერგა მიიღო სახელწოდება *ARPANET*.

ქსელი *ARPANET* 70-ან წლებში ნელა ვითარდებოდა. განვითარება ძირითადად რეგიონალური ქსელების მიერთების ხარჯზე ხდებოდა, რომლებიც ქმნიდნენ *ARPANET*-ის საერთო სტრუქტურას რეგიონალურ ან ლოკალურ მასშტაბში. *ARPANET*-ის ძირითად გაცხადებულ ამოცანად ერთიან მეცნიერულ-ტექნიკურ პროექტებზე მომუშავე კოლექტივთა ჯგუფების კოორდინაცია გახდა, ხოლო ძირითად დანიშნულებას მეცნიერული და საპროექტო-საკონსტრუქტორო დოკუმენტების ფაილების და ელექტრული ფოსტის გაცვლა წარმოადგენდა. მათე დროს არ წყდებოდა მუშაობა გაუცხადებელ ამოცანაზე - ახალი ქსელური

პროტოკოლების დამუშავებაზე, რომლებიც უზრუნველყოფდა გლობალური ქსელის სიცოცხლისუნარიანობას ბირთვული კონფლიქტების დროსაც.

ინტერნეტის დაბადების მეორე თარიღად 1983წ. ითვლება, როდესაც კომპიუტერული ქსელების პროგრამულ უზრუნველყოფაში რევოლუციური ცვლილებები მოხდა. გლობალური ქსელების მდგრადობის პრობლემა გადაწყდა *TCP/IP* პროტოკოლის დანერგვით, რომელიც დღესაც საფუძვლად უდევს საერთაშორისო ქსელის მუშაობას. ამ ამოცანის გადაწყვეტის შემდეგ სამმართველომ *DARPA* შეწყვიტა თავისი მონაწილეობა პროექტში და ქსელის მართვა გადასცა ნაციონალურ სამეცნიერო ფონდს (*NSF*), რომელიც აშშ-ში იგივე როლს ასრულებს, რასაც ჩვენში მეცნიერებათა აკადემია. ამგვარად, 1983 წელს წარმოიქმნა გლობალური ქსელი *NSFNET*. 80-იანი წლების შუა პერიოდში მასთან აქტიურად დაიწყო მიერთება სხვა ქვეყნების აკადემიურმა და სამეცნიერო ქსელებმა, მაგალითად დიდი ბრიტანეთის აკადემიურმა ქსელმა *JANET (Joined Academic Network)*.

წლები, როდესაც გლობალურ ქსელს ხელმძღვანელობდა აშშ-ს ნაციონალური სამეცნიერო ფონდი ისტორიაში შევიდა, როგორც ქსელების კომერციალიზაციის მცდელობის ეპოქა. ქსელი ფინანსდებოდა სამთავრობო სახსრებით. ნაციონალური სამეცნიერო ფონდი ანაწილებდა მას კვანძებს შორის და მატერიალურად სჯიდა მათ, ვინც ცდილობდა გვერდითი შემოსავლები ქონოდა ქსელიდან. ამასთან ერთად, *TCP/IP* პროტოკოლის დანერგვის შემდეგ ქსელის გნვითარება მნიშვნელოვნად დაჩქარდა, *NSF* უკვე ვეღარ ასწრებდა

თვითოეული კვანძის საქმიანობის თვალყურის დევნებას, ხოლო უცხოური სექტორების მიერთებით მისი როლი სიმბოლური გახდა.

80-იანი წლების მეორე ნახევარში საერთაშორისო ქსელის დაყოფა მოხდა დომენებად კუთვნილების პრინციპის მიხედვით. დომენი gov - ფინანსდებოდა მთავრობის სახსრებით, დომენი SCI - სამეცნიერო წრეების სახსრებით, დომენი edu - განათლების სისტემის სახსრებით, ხოლო დომენი com - (კომერციული) არ ფინანსდებოდა არავისგან, ანუ მისი კვანძები უნდა განვითარებულიყო საკუთარი რესურსების ხარჯზე. სხვა ქვეყნების ნაციონალური ქსელები განიხილებოდნენ, როგორც ცალკეული დომენები. მაგალითად, uk - დიდი ბრიტანეთის დომენი, ru - რუსეთის დომენი.

როდესაც 80-იანი წლების მეორე ნახევარში ჩამოყალიბდა და ამუშავდა დომენების სახელების სისტემა (*DNS, Domain Name System*), აშშ-ს ნაციონალურმა სამეცნიერო ფონდმა დაკარგა კონტროლი ქსელის განვითარებაზე. ამ დროს გაჩნდა *ინტერნეტის*, როგორც თვითგანვითარებადი, დეცენტრალიზებული იერარქიული სტრუქტურის ცნება. თუ *ARPENET* და *NSNET* ქსელების დროს ქსელი ფინანსდებოდა ზემოდან ქვემოთ, ახლა კი იგი ფინანსდება პერიფერიებიდან, ქვემოდან ზევით - საბოლოო მომხმარებელიდან ქსელების ძირითადი მფლობელებისაკენ.

1.4 ინტერნეტის ძირითადი ცნებები.

ზოგადად, ინტერნეტი არის ქსელების *გაერთიანება*. მაგრამ, ბოლო ხანს ამ სიტყვამ უფრო ფართო აზრი შეიძინა - *საერთაშორისო კომპიუტერული ქსელი*. ინტერნეტი ფიზიკური გაგებით შეიძლება განვიხილოთ როგორც ყველა შესაძლო

კავშირის არსებით ერთმანეთთან დაკავშირებული მილიონობით კომპიუტერი, მაგრამ ინტერნეტის ასეთი „ფიზიკური“ ხედვა ძალზე ვიწროა, უმჯობესია განვიხილოთ იგი როგორც რაიმე ინფორმაციული სივრცე.

ინტერნეტი არ არის კომპიუტერებს შორის პირდაპირი შეერთებების ერთობლიობა. მაგალითად, თუ სხვადასხვა კონტინენტზე განლაგებული ორი კომპიუტერი ცვლიან მონაცემებს ინტერნეტში სულაც არ ნიშნავს, რომ მათ შორის არსებობს ერთი პირდაპირი შეერთება. მონაცემები, რომლებსაც ისინი უგზავნიან ერთმანეთს იყოფა ცალკეულ პაკეტებათ და უფრო მეტიც, ერთი შეტყობინების სხვადასხვა პაკეტებმა კავშირის ერთი სეანსის დროს შეიძლება გაიარონ სხვადასხვა მარშუტი. რა მარშუტითაც არ უნდა იმოძრაონ მონაცემთა პაკეტებმა, მიაღწევენ რა ისინი დანიშნულების ადგილს გაერთიანდებიან მთლიან დოკუმენტად. ამასთან, გვიან გაგზავნილი მონაცემთა პაკეტები შეიძლება მივიდეს უფრო ადრე, მაგრამ ეს ხელს არ შეუშლის სწორად აიკინძოს დოკუმენტი, რადგანაც თვითოეულ პაკეტს აქვს თავისი სპეციალური ნიშანი (მარკერი).

ამგვარად, ინტერნეტი წარმოადგენს თითქოს „სივრცეს“, რომლის შიგნითაც ხორციელდება მონაცემების უწყვეტი ცირკულაცია. ამ გაგებით იგი შეიძლება შევადაროთ ტელე და რადიო ეთერს, თუმცა არის არსებითი განსხვავება, რომელიც მდგომარეობს იმაში, რომ ეთერში არავითარი ინფორმაცია არ შეიძლება შეინახოს, ხოლო ინტერნეტში ინფორმაცია გადაადგილდება ქსელის კვანძების შემადგენელ კომპიუტერებს

შორის და ინახება მათ ხისტ დისკებზე მოცემული დროის განმავლობაში.

TCP/IP პროტოკოლების სტეკი. TCP/IP პროტოკოლმა მნიშვნელოვანი როლი დაიმკვიდრა ინტერნეტის ჩამოყალიბებაში. TCP/IP პროტოკოლი ტექნიკური გაგებით არის არა ერთი ქსელური პროტოკოლი, არამედ ორი სხვადასხვა დონეზე მყოფი პროტოკოლი (ე.წ. პროტოკოლების სტეკი). პროტოკოლი *TCP-სატრანსპორტო დონის პროტოკოლია*, ის მართავს მონაცემების გადაცემის პროცესს. პროტოკოლი *IP - სამისამართოა*. ის მიეკუთვნება *ქსელურ დონეს* და განსაზღვრავს *თუ სად ხდება გადავზავნა*.

პროტოკოლი TCP. TCP პროტოკოლის თანახმად გადასავზავნი მონაცემები „იჭრება“ მცირე პაკეტებად, თვითოეული პაკეტი მოინიშნება ისეთნაირად, რომ მასში იყოს მიმღების კომპიუტერზე დოკუმენტის სწორი აწყობისათვის საჭირო მონაცემები.

ერთი ფიზიკური შეერთებით დაკავშირებულ ორ კომპიუტერს შეუძლია ერთდროულად რამოდენიმე TCP-შეერთების მომსახურება. ასე მაგალითად, ორ შუალედურ ქსელურ სერვერს ერთდროულად შეუძლია ერთი კავშირის არხით, გადასცეს ერთმანეთს ორივე მიმართულებით მრავალი TC - პაკეტები მრავალრიცხოვანი კლიენტებისაგან.

როდესაც ვმუშაობთ ინტერნეტში, ერთადერთი სატელეფონო ხაზით შეგვიძლია ერთდროულად მივიღოთ დოკუმენტები ამერიკიდან, ავსტრალიიდან და ევროპიდან. თვითოეული დოკუმენტის პაკეტები მიიღება ცალცალკე, დროში

განაწილებული და მიღებისთანავე ერთიანდებიან სხვადასხვა დოკუმენტებში.

IP-პროტოკოლი. *IP (Internet Protokol)* სამისამართო პროტოკოლია და მისი არსი მდგომარეობს იმაში, რომ საერთაშორისო ქსელის თვითოეულ მონაწილეს უნდა ქონდეს თავისი უნიკალური მისამართი (*IP-მისამართი*). ამის გარეშე შეუძლებელია *TCP* - პაკეტების ზუსტად დანიშნულების ადგილზე მიტანა. ეს მისამართი მარტივად ოთხი ბაიტით გამოიხატება, მაგალითად: 195.38.46.11. *IP* - მისამართი ორგანიზებულია ისე, რომ თვითოეულ კომპიუტერს, რომლის გავლითაც გადაეცემა რომელიმე *TCP* - პაკეტი, შეუძლია ამ ოთხი რიცხვით განსაზღვროს რომელ უახლოეს „მეზობელს“ უნდა გადაეგზავნოს პაკეტი, რომ ის მოხვდეს „ახლოს“ მიმღებთან ბოლო გადაგზავნის შემდეგ *TCP* - პაკეტი აღწევს ადრესატამდე.

სიტყვა „ახლო“-ში არ იგულისხმება გეოგრაფიული „ახლო“. მხედველობაშია კავშირის პირობები და ხაზის გამტარუნარიანობა. სხვადასხვა კონტინენტზე განთავსებული, მაღალმწარმოებლური კოსმოსური კავშირის არხით დაკავშირებული ორი კომპიუტერი ითვლება უფრო „ახლო“ ერთმანეთთან, ვიდრე უბრალო ტელეფონის ხაზით დაკავშირებული ორი მეზობელი დასახლების კომპიუტერები. საკითხს რა ჩაითვალოს „ახლო“ და რა „შორს“ წყვეტს სპეციალური საშუალება-*მარშუტიზატორი*. ქსელში მარშუტიზატორის როლს ჩვეულებრივად ასრულებს სპეციალიზირებული კომპიუტერი ან კვანძის სერვერებში მომუშავე სპეციალური პროგრამები. ვინაიდან ერთი ბაიტი მოიცავს 256 სხვადასხვა მნიშვნელობას, თეორიულად ოთხი ბაიტით შეიძლება გამოვსახოთ ოთხ მილიარდზე მეტი უნიკალური

IP-მისამართი. (256⁴ - რამოდენიმე სასამსახურო მისამართის გამოკლებით). პრაქტიკაში, ზოგიერთი ტიპის ლოკალური ქსელების თავისებურებების გათვალისწინებით შესაძლო მისამართების რაოდენობა ორ მილიარდს შეადგენს. ეს საკმაოდ დიდი რიცხვია, მაგრამ მისი შემოსაზღვრულობა სულ უფრო შესამჩნევი ხდება. როგორც კი ინტერნეტში ფართოდ შემოვა კავშირის მობილურ საშუალებებთან (ფიჭური რადიო-ტელეფონებით) ურთიერთქმედების სამსახურები, თავს იჩენს *IP*-სამისამართო ველების სიმცირე.

1.5 ინტერნეტის სამსახურები.

ინტერნეტში მუშაობაზე ან ინტერნეტის გამოყენებაზე საუბრისას ლაპარაკია არა მთლიანობაში ინტერნეტზე არამედ მისი მრავალრიცხოვანი სამსახურებიდან ერთერთზე. კონკრეტული მიზნებისა და ამოცანებიდან გამომდინარე ქსელის კლიენტები იყენებენ იმ სამსახურებს, რომლებიც მათთვისაა აუცილებელი.

მარტივი გაგებით სამსახური არის პროგრამების წყვილი, რომლებიც ერთმანეთთან ურთიერთქმედებენ განსაზღვრული წესებით-*პროტოკოლებით*. ამ წყვილის ერთ-ერთ პროგრამას ეწოდება *სერვერი*, ხოლო მეორეს-*კლიენტი*. შესაბამისად როდესაც საუბრობენ ინტერნეტის სამსახურების მუშაობაზე, საქმე ეხება სერვერული მოწყობილობებისა და პროგრამული უზრუნველყოფის ურთიერთქმედებას კლიენტის მოწყობილობასა და პროგრამულ უზრუნველყოფასთან.

სხვადასხვა სამსახურებს სხვადასხვა პროტოკოლები აქვთ. ინტერნეტის სამსახურების პროტოკოლებს *დანართ პროტოკოლებს* უწოდებენ. მათი დაცვა და მომსახურება

ხორციელდება სპეციალური პროგრამების მუშაობით. მაშასადამე, იმისათვის რომ ვისარგებლოთ ინტერნეტის რომელიმე სამსახურით, აუცილებელია დავაყენოთ კომპიუტერზე კლიენტის პროგრამა, რომელიც უზრუნველყოფს მოცემული სამსახურის პროტოკოლით მუშაობას და დაფუკავშიროთ იგი სერვერის პროგრამას. მაგალითად, ფაილების გადასაცემად ინტერნეტში გამოიყენება სპეციალური პროტოკოლი *FTP (File Transfer Protocol)*. შესაბამისად ინტერნეტიდან ფაილის მისაღებად აუცილებელია:

- ✓ გვქონდეს კომპიუტერზე პროგრამა, რომელიც წარმოადგენს *FTP-ის* კლიენტს (*FTP-კლიენტი*);
- ✓ დავამყაროთ კავშირი სერვერთან, რომელიც უზრუნველყოფს *FTP-ის* მომსახურებას (*FTP-სერვერი*).

ელექტრონული ფოსტით სარგებლობისათვის კი, აუცილებელია შეტყობინებების მიღებისა და გაგზავნის პროტოკოლის დაცვა. ამისათვის უნდა გვქონდეს პროგრამა (*ფოსტის კლიენტი*) და განვახორციელოთ კავშირი *საფოსტო სერვერთან*. ასევე მყარდება კავშირი სხვა სამსახურებთანაც.

ტერმინალის რეჟიმი. ისტორიულად ერთ-ერთ ყველაზე ადრეულ სამსახურს წარმოადგენს კომპიუტერის დაშორებული მართვა *Telnet*. მიუხედავად იმისა რა დაშორებულ კომპიუტერს ამ სამსახურის პროტოკოლით, შესაძლებელია მისი მუშაობის მართვა. ასეთ მართვას აგრეთვე *ტერმინალურს* უწოდებენ. წარსულში ამ სამსახურს ფართოდ იყენებდნენ დაშორებულ გამოთვლით ცენტრებში რთული გამოთვლების ჩასატარებლად. თუ რთული გამოთვლებისათვის პერსონალური კომპიუტერის ერთი კვირის განუწყვეტელი მუშაობა იყო საჭირო, ხოლო დაშორებულ სუპერ კომპიუტერებზე სულ რამოდენიმე წუთი,

მაშინ პერსონალურ კომპიუტერს იყენებდნენ მხოლოდ დაშორებულ კომპიუტერებში მონაცემების შესატანად და გამოთვლების შედეგების მისაღებად.

ამჟამად, პერსონალური კომპიუტერების სიმძლავრეების სწრაფი ზრდის გამო, მსგავს მომსახურებაზე მოთხოვნა შემცირდა, თუმცა *Telnet* სამსახური აგრძელებს ინტერნეტში თავის არსებობას. ხშირად *Telnet* პროტოკოლებს იყენებენ დაშორებული ტექნიკური ობიექტების სამართავად, მაგალითად: ტელესკოპები, ვიდეოკამერები, საწარმოო რობოტები, ავტომატიზირებული საწყოები, აგრეთვე სავაჭრო ავტომატებიც.

ყოველი სერვერი, რომელიც ასრულებს *Telnet*-სამსახურს, ჩვეულებრივად თავაზობს თავის კლიენტ-დანართს. ის უნდა მიიღოს ქსელით (მაგალითად *FTP*-პროტოკოლით), დააყენოს თქვენს კომპიუტერზე, დაუკავშირდეთ სერვერს და იმუშაოთ დაშორებული მოწყობილობით. უმარტივესი კლიენტი-*Telnet* შედის ოპერაციული სისტემის *Windows* -ის შემადგენლობაში (ფაილი *Telnet.exe*).

ელექტრონული ფოსტა (E-Mail) ეს სამსახურიც ერთ-ერთ ადრეულ სამსახურს წარმოადგენს. ინტერნეტში მას უზრუნველყოფს სპეციალური *საფოსტო სერვერი* და არა სპეციალური გამოყოფილი კომპიუტერი. აქ და შემდეგშიც სერვერის ქვეშ შეიძლება იგულისხმებოდეს პროგრამული უზრუნველყოფა. ამგვარად, ინტერნეტის ერთი საკვანძო კომპიუტერი შეიძლება ასრულებდეს რამოდენიმე სერვერის ფუნქციებს და უზრუნველყოფდეს სხვადასხვა სამსახურების სამუშაოს, ამასთანავე იგი რჩებოდეს უნივერსალურ

კომპიუტერად, რომელზედაც შეიძლება შესრულდეს გამოთვლითი ტექნიკისათვის დამახასიათებელი სხვა ამოცანები.

საფოსტო სერვერები შეტყობინებებს იღებენ კლიენტებისაგან და გადასცემენ მათ ადრესატების საფოსტო სერვერებს, სადაც ეს შეტყობინებები გროვდება. ადრესატისა და მისი საფოსტო სერვერის დაკავშირების შემდეგ შემოსული შეტყობინებები ავტომატურად გადაეცემა ადრესატის კომპიუტერს.

საფოსტო სამსახური დამყარებულია ორი პროტოკოლიდანართის გამოყენებაზე: *SMTP* და *POP3*. პირველი პროტოკოლით ხდება კორესპონდენციების გაგზავნა კომპიუტერიდან სერვერზე, ხოლო მეორეთი - შემოსული შეტყობინებების მიღება. არსებობს კლიენტის მრავალი პროგრამა, მაგალითად *Microsoft Outlook Express*, რომელიც შედის ოპერაციული სისტემის Windows-ის სტანდარტულ კომპლექტში. უფრო მძლავრი პროგრამაა *Microsoft Outlook 2000, 2003*, რომელიც Windows 2000, 2003-ის სტანდარტულიდანართია. მათში გარდა ელექტრული ფოსტისა ინტეგრირებულია საქმეთწარმოების სხვა საშუალებები. სპეციალიზირებული საფოსტო პროგრამებიდან კარგი პოპულარობა აქვთ პროგრამებს *The Bat!*, *Eudora*, *Pegasus mail*.

დაგზავნის სიები (Mailing List) ჩვეულებრივი ელექტრონული ფოსტა გულისხმობს მიმოწერაში ორი პარტნიორის არსებობას. თუ პარტნიორები არ არიან, მაშინ ჩვენს მისამართზე ინფორმაციის საკმარისად დიდი ნაკადი შეიძლება ვუზრუნველყოთ დაგზავნის სიებზე ხელმოწერით. ეს სპეციალური თემატური სერვერებია, რომლებიც აგროვებენ ინფორმაციას განსაზღვრულ თემებზე და გადაგზავნიან ხელმოწერის კომპიუტერზე ელექტრონული ფოსტის შეტყობინებების სახით.

დაგზავნის სიების თემა შეიძლება ნებისმიერი იყოს, მაგალითად, უცხო ენების შესწავლის საკითხები, კომერციული და ფინანსური მიმოხილვები, გამოთვლითი ტექნიკის ახალი პროგრამული და აპარატული საშუალებების პრეზენტაცია და სხვა. მრავალი ტელეკომპანიები ქმნიან თავის კვანძებზე დაგზავნის სიებს, რომლის საშუალებითაც უგზავნიან კლიენტებს ტელეპროგრამების ანოტირებულ მიმოხილვას. დაგზავნის სიები საშუალებას იძლევიან ეფექტურად გადავწყვიტოთ მონაცემების რეგულარული მიწოდების საკითხები.

ტელეკომფერენციების სამსახური (Usnet). ეს სამსახური ელექტრონული ფოსტის ცირკულარული დაგზავნის მსგავსია, რომლის დროსაც ერთი შეტყობინება გაეგზავნება არა ერთ არამედ კორესპონდენტების მრავალ ჯგუფს (ასეთ ჯგუფებს ტელეკომფერენციებს ან სიახლეების ჯგუფს უწოდებენ).

ელექტრონული ფოსტის ჩვეულებრივი შეტყობინება გამგზავნიდან მიმღებს დაეგზავნება სერვერების ვიწრო წრედით. ამასთან შუაღედ სერვერებზე მისი შენახვა არ ივარაუდება. სიახლეთა ჯგუფის სერვერზე მიმართული შეტყობინება გაიგზავნება მასთან დაკავშირებულ ყველა სერვერზე თუ მოცემული შეტყობინება მათზე ჯერ კიდევ არ არის მიღებული. შემდეგში პროცესი მეორდება.

თვითოველ სერვერზე მისული შეტყობინება ინახება შეხლდელი დროის განმავლობაში (ჩვეულებრივად კვირა) და ყველა მსურველს შეუძლია გაეცნოს მას ამ დროის განმავლობაში. ვრცელდება რა ყოველ მხარეს შეტყობინება დღე-ღამეზე ნაკლებ დროში მოივლის მთელ დედამიწას. შემდეგ გავრცელება ნელდება, ვინაიდან სერვერზე, რომელსაც მიღებული

აქვს მოცემული შეტყობინება განმეორებით გადაგზავნა აღარ ხდება.

ყოველდღიურად მსოფლიოში მილიონებით შეტყობინება იქმნება სიახლეთა ჯგუფისათვის. ნამდვილად სასრუგებლო ინფორმაციის ამორჩევა ამ მასივში პრაქტიკულად შეუძლებელია. ამიტომ ტელეკომფერენციების მთელი სისტემა დაყოფილია თემატურ ჯგუფებად. დღეს მსოფლიოში 50 000-მდე სიახლეების თემატურ ჯგუფს ითვლიან. ისინი მოიცავენ მასებისათვის მტნაკლებად საინტერესო თემებს. განსაკუთრებული პოპულარობით სარგებლობს გამოთვლითი ტექნიკის სიახლეთა ჯგუფი.

სიახლეთა ჯგუფის გამოყენების ძირითადი წესი მდგომარეობს იმაში, რომ მივმართავთ რა მთელ მსოფლიოს დავსვათ ჩვენთვის მნიშვნელოვანი საკითხი და მივიღოთ პასუხი ან რჩევა მათგან ვინც უკვე გაერკვა ამ საკითხში. ამასთან მნიშვნელოვანია თვალყური ვადევნოთ, რომ საკითხის შინაარსი შეესაბამებოდეს მოცემული ტელეკომფერენციის თემას. მსოფლიოს მრავალი კვალიფიციური სპეციალისტები (მეცნიერები, ექიმები, პედაგოგები, იურისტები, მწერლები, ეკონომისტები, პროგრამისტები და სხვა) რეგულარულად ათვალიერებენ ტელეკომფერენციის შეტყობინებებს მათი საქმიანობის სფეროს შესაბამის ჯგუფებიდან. ასეთ დათვალიერებას ინფორმაციის *მონიტორინგს უწოდებენ*. ინფორმაციის რეგულარული მონიტორინგი საშუალებას აძლევს სპეციალისტებს ზუსტად იცოდნენ თუ რა სიახლეებია მსოფლიოში მათი სპეციალობით, რა პრობლემები აწუხებს ადამიანების დიდ ჯგუფს და რაზე გაამახვილონ თავის საქმიანობაში ყურადღება.

შეტყობინების გაგზავნისას ტელეკომფერენციაში მიღებულია ადრესატის ელექტრონული ფოსტის მისამართის მითითება პასუხის მისაღებად. იმ შემთხვევაში, როდესაც არის ელექტრონული „ფოსტის ყუთის“ კორექსონდენციებით გადავსების საშიშროება, რომელიც უშუალოდ საწარმოო საქმიანობას არ მიეკუთვნება, საქმიანი მიმოწერისათვის განკუთვნილი ძირითადი მისამართის ნაცვლად მიუთითებენ დამატებით მისამართს. როგორც წესი, ასეთ მისამართს ქირაობენ ერთერთ უფასო ანონიმური საფოსტო სამსახურის სერვერზე. მაგალითად: www.hotmail.com.

დიდი მოცულობის შეტყობინებები სიხლეტა ჯგუფში მნიშვნელოვნად აძნელებს მათ მიზანმიმართულ მონიტორინგს, ამიტომ ზოგიერთ ჯგუფში წინასწარ ხდება იმ უსარგებლო ინფორმაციის „გაცხრილვა“, რომელიც არ ეხება კონფერენციის თემას. ასეთ კომფერენციებს *მოდერირებულს* უწოდებენ. *მოდერატორის* ფუნქციას შეიძლება ასრულებდეს არა მხოლოდ ადამიანი, არამედ პროგრამაც, რომელიც ფილტრავს შეტყობინებებს გასაღები სიტყვის მიხედვით. ამ შემთხვევაში საუბრობენ *ავტომატურ მოდერაციაზე*.

ტელეკომფერენციების სამსახურებთან სამუშაოდ არსებობენ კლიენტის სპეციალური პროგრამები. მაგალითად დანართი *Microsoft Outlook Express*, რომელიც გარდა ფოსტისა ტელეკომფერენციების სამსახურთან მუშაობის საშუალებასაც იძლევა. დასაწყისში აუცილებელია პროგრამის გამართვა სიხლეტა ჯგუფის სერვერთან სამუშაოდ, კერძოდ ფორმდება „ხელმოწერა“ გარკვეულ ჯგუფებზე და პერიოდულად მიიღებთ შეტყობინებებს ამ ჯგუფის თემების შესახებ. სიტყვა

„ხელშეკრულება“ კლიენტის მხრიდან არ ითვალისწინებს არავითარ ვალდებულებებს ან გადასახადს. ეს მხოლოდ შეტყობინებაა სერვერისათვის, რომ მითითებულ თემაზე შეტყობინებები უნდა გაუგზავნოს მითითებულ კლიენტს და არა სხვას. ხელმოწერის გაუქმება ან თემის შეცვლა შესაძლებელია ნებისმიერ დროს.

World Wide Web (WWW) სამსახური. WWW სამსახური ყველაზე პოპულარულია თანამედროვე ინტერნეტში. მას ხშირად აიგივებენ ინტერნეტთან, თუმცა ის ინტერნეტის ერთერთი სამსახურია.

World Wide Web არის ურთიერთდაკავშირებული ელექტრონული დოკუმენტებისაგან შემდგარი ერთიანი ინფორმაციული სივრცე, რომელიც ინახება *Web-სერვერზე*. *Web-სივრცის* შემადგენელ ცალკეულ დოკუმენტებს *Web-გვერდებს* უწოდებენ. ამ დროისათვის უნიკალური *Web-გვერდების* რაოდენობა ორ მილიარდზე მეტია, ამასთან ზრდის ტემპი ისეთია, რომ ეს მონაცემები ძალზე სწრაფად ძველდება.

თემატურად გაერთიანებულ *Web-გვერდებს Web-კვანძებს* უწოდებენ. ერთი ფიზიკური *Web-სერვერი* შეიძლება შეიცავდეს საკმარისად ბევრ *Web-კვანძებს*, რომელთაგან თვითოეულს, როგორც წესი, გამოყოფილი აქვს ცალკე კატალოგი სერვერის ხისტ დისკზე. *Web-გვერდი* ჩვეულებრივი ტექსტური დოკუმენტებისაგან იმით განსხვავდება, რომ ისინი გაფორმებულია რომელიმე კონკრეტულ მატარებელზე დამოუკიდებლად. მაგალითად, ქაღალდზე დაბეჭდილი დოკუმენტის გაფორმება დამოკიდებულია საბეჭდი ქაღალდის პარამეტრებზე, რომელსაც აქვს განსაზღვრული სივანე, სიმაღლე და ველების ზომები.

ელექტრონული Web-დოკუმენტები კი განკუთვნილია კომპიუტერის ეკრანზე დასათვალიერებლად, ამასთან წინასწარ არაა ცნობილი რომელ კომპიუტერზე, უცნობია ეკრანის ზომები, ფერისა და გრაფიკული გამტარიანობის პარამეტრები, უცნობია აგრეთვე კლიენტის კომპიუტერზე დაყენებული ოპერაციული სისტემა. ამიტომ, Web-დოკუმენტს არ შეიძლება ქონდეს „ხისტი“ დაფორმატება. დოკუმენტის გაფორმება კლიენტის კომპიუტერზე უშუალოდ მისი გამოტანისას ხდება იმ პროგრამის შესაბამისად რომელიც ასრულებს დათვალიერების ოპერაციას.

Web-გვერდების დასათვალიერებელ პროგრამებს *ბრაუზერებს* უწოდებენ. ლიტერატურაში შეიძლება შევხვდეთ აგრეთვე არ შემდგარ ტერმინს „*მიმომხილველი*“. ყველა შემთხვევაში საუბარია *Web-დოკუმენტის დათვალიერების რაიმე საშუალებაზე (პროგრამაზე)*.

ბრაუზერი ასრულებს დოკუმენტის ეკრანზე გამოსახვას იმ ბრძანებების მიხედვით რომელიც დოკუმენტის ავტორმა ჩადო ტექსტში, (თუ ავტორი იყენებს Web-დოკუმენტის გაფორმების ავტომატურ საშუალებებს, აუცილებელი ბრძანებები ავტომატურად იდება ტექსტში). ასეთ ბრძანებებს „*ტეგებს*“ (ნიშნულებს) უწოდებენ. ჩვეულებრივი ტექსტისაგან ისინი იმით განსხვავდებიან, რომ მოთავსებულია კუთხურ ფრჩხილებში. ტეგების უმრავლესობა წყვილად გამოიყენებიან: *გამღები ტეგი და დამხურავი ტეგი*. დამხურავი ტეგი იწყება „*<*“ სიმბოლოთი.

მაგ: <CENTER> ეს ტექსტი განთავსდება ეკრანის ცენტრში </CENTER>

<P ALIGN = „LEFT“> ეს ტექსტი განთავსდება ეკრანის მარცხენა საზღვარზე </P>.

<P ALIG = „RIGHT“> ეს ტექსტი განთავსდება ეკრანის მარჯვენა საზღვარზე </P>.

როულ ტეგებს გარდა *გახაღები* სიტყვისა აქვთ დამატებითი პარამეტრები და ატრიბუტები, რომლებიც აზუსტებენ მათი გამოყენების წესებს. ტეგების ჩაწერის წესები შეტანილია დაპროგრამების ენების მსგავს, განსაკუთრებული მონიშვნის ენის სპეციფიკაციაში. ამ ენას ჰიპერტექსტის მონიშვნის ენას *HTML (Hiper Text Markup Language)* უწოდებენ და იგი განკუთვნილია ჰიპერტექსტური დოკუმენტების მოსამზადებლად. მაშასადამე Web-დოკუმენტი წარმოადგენს ჩვეულებრივ ტექსტურ დოკუმენტს, რომელიც მონიშნულია *HTML* ტეგებით. ასეთ დოკუმენტებს *HTML-დოკუმენტებს* ან *დოკუმენტებს HTML ფორმატში* უწოდებენ.

ბრაუზერის საშუალებით *HTML-დოკუმენტის* ეკრანზე გამოსახვისას ეკრანზე ტეგები არ ჩანან, ვხედავთ მხოლოდ დოკუმენტის შემადგენელ ტექსტს. მაგრამ ამ ტექსტის გაფორმება (განთავსება, ფერი, ზომები, შრიფტის მოსაზულობა და სხვა) სრულდება ტექსტში ჩადებული ტეგების შესაბამისად.

არსებობენ ტექსტში გრაფიკული და მულტიმედიის ობექტების განთავსების (მუსიკა, ხმები, ვიდეოკლიპები) სპეციალური ტეგები. შეხვედბა რა ბრაუზერი ასეთ ტეგს, ტეგთან დაკავშირებულ ფაილის მისაღებად მიაკითხავს სერვერს და წარმოადგენს მას ტეგის მოცემული პარამეტრებისა და ატრიბუტების შესაბამისად, რის შედეგადაც ვხედავთ ილუსტრაციებს ან ვისმენთ ხმებს.

ბოლო წლებში, *Web-დოკუმენტებში* ფართო გამოყენება მოიპოვეს ეგრეთ წოდებულმა *აქტიურმა კომპონენტებმა*. ეს იგივე დოკუმენტებია, მაგრამ ისინი შეიცავევენ არა მარტო ტექსტს, ან

გრაფიკულ და მულტიმედიურ მონაცემებს, არამედ პროგრამულ კოდებსაც და შეუძლიათ არა უბრალოდ აისახონ კლიენტის კომპიუტერის ეკრანზე, არამედ შეასრულონ პროგრამაში ჩადებული სამუშაო.

HTML-ის ტეგების საშუალებით ტექსტში გრაფიკული ან სხვა ობიექტების ჩართვის შესაძლებლობა ყველაზე ეფექტურია *Web*-გვერდების გაფორმების თვალსაზრისით, მაგრამ არა ყველაზე მნიშვნელოვანი თვითონ *World Wide Web* იდეის თვალსაზრისით. *HTML*-ის ტეგების საშუალებით განხორციელებული *Web*-გვერდების ყველაზე მნიშვნელოვანი თვისება *ჰიპერტექსტური მიმართება*ა. ტექსტის ნებისმიერ ფრაგმენტთან ან მაგალითად სურათთან ტეგების საშუალებით შეიძლება დაუკავშიროთ სხვა *Web*-დოკუმენტი, ანუ დავამყაროთ ჰიპერმიმართვა. ამ შემთხვევაში იმ ტექსტზე ან სურათზე, რომელიც ჰიპერმიმართვას წარმოადგენს, მაუსის მარცხენა ღილაკის დაწკაპუნებით იგზავნება ახალი დოკუმენტის მიღების მოთხოვნა შესაბამის სერვერზე. ამ დოკუმენტს კი თავის მხრივ, შეიძლება ქონდეს ჰიპერმიმართვა სხვა დოკუმენტზე და ა.შ..

ამრიგად, *WWW* სერვერზე შენახული დიდი რაოდენობის ჰიპერტექსტური ელექტრონული დოკუმენტების ერთობლიობა წარმოქმნიან დოკუმენტების თავისებურ ჰიპერსივრცეს, რომელთა შორის შესაძლებელია გადაადგილება. *Web*-სივრცის დოკუმენტებს შორის თავისუფლად გადაადგილებას გაცნობითი ხასიათის დათვალიერების მიზნით *Web*-სერფინგს უწოდებენ, ხოლო მიზნობრივ გადაადგილებას ინფორმაციის მოძებნის მიზნით *Web-ნავიგაციას* უწოდებენ.

ინტერნეტის ფიზიკურ სერვერებზე შენახულ მილიარდობით დოკუმენტებს შორის ჰიპერტექსტური კავშირი წარმოადგენს *World Wide Web*-ის ლოგიკური სივრცის არსებობის საფუძველს. მაგრამ ასეთი კავშირი ვერ იარსებებდა თუ ამ სივრცის ყოველ დოკუმენტს არ ექნებოდა უნიკალური მისამართი. ნებისმიერი ფაილის სახელი საერთაშორისო ქსელის მასშტაბით განისაზღვრება *რესურსის უნიფიცირებული მაჩვენებლით - URL (Inform Resource Lokator)*.

URL მისამართი შედგება სამი ნაწილისაგან.

1. სამსახურის მითითება, რომელიც ახორციელებს მოცემულ რესურსთან მიღწევას (მოცემული სამსახურის შესაბამისი გამოყენებითი პროტოკოლის სახელი). მაგალითად *www* სამსახურისათვის გამოყენებითს წარმოადგენს *HTTP (Hyper Text Transler Protokol - ჰიპერტექსტის გადაცემის პროტოკოლი)*. პროტოკოლის სახელის შემდეგ ისმება ორი წერტილი (:) და ორი ნიშანი „/“ (დახრილი ხაზი):

http:// . . .

2. კომპიუტერის (სერვერის) *დომენური სახელის* მითითება, რომელზეც ინახება მოცემული რესურსი.

http://www.pcworld.com ...

3. მოცემულ კომპიუტერზე ფაილთან შედწვევის სრული გზის მითითება. გამყოფ ნიშნად გამოიყენება სიმბოლო „/“ (დახრილი ხაზი)

http://www.psworld.com/software_lib/index.html

URL მისამართის ჩაწერისას მნიშვნელოვანია სიმბოლოების რეგისტრების ზუსტი დაცვა. MS DOS-ში და Windows-

ში მუშაობის წესებისაგან განსხვავებით, ინტერნეტში ხელნაწერი და ბეჭდური ასოები სხვადასხვად ითვლებიან.

სწორედ *URL* ფორმით უკავშირებენ რესურსის მისამართს ჰიპერტექსტურ მიმართვებთან *Web*-გვერდებზე. ჰიპერმიმართვაზე მაუსის დაწკაპუნებით ბრაუზერი სერვერს უგზავნის მოთხოვნას იმ რესურსის მოძებნისა და გადმოგზავნის შესახებ, რომელიც მითითებულია მიმართვაში. თუ რაიმე მიზეზის გამო რესურსი ვერ მოიძებნა, გაიცემა შეტყობინება იმაზე, რომ რესურსი მიუღწეველია (შესაძლებელია რომ სერვერია გათიშული ან შეცვლილია რესურსის მისამართი).

დომენების (DNS) სახელების სამსახური. როდესაც ვსაუბრობდით ინტერნეტის პროტოკოლებზე, ავლინებდით, რომ, ნებისმიერი კომპიუტერის ან ლოკალური ქსელის მისამართი ინტერნეტში შეიძლება აღინიშნოს ოთხი ბაიტით, მაგალითად ასე: 195·28·132·97

ასევე განვაცხადეთ, რომ თვითოეულ კომპიუტერს აქვს უნიკალური დომენური სახელი, მაგალითად ასეთი www.peworld.com

ხომ არ არის აქ წინააღმდეგობა? არავითარი წინააღმდეგობა აქ არ არის, რადგანაც ეს ქსელის ერთი და იგივე კომპიუტერის მისამართის ჩაწერის ორი სხვადასხვა ფორმაა. ადამიანისათვის მოუხერხებელია რიცხვით წარმოდგენილ *IP*-მისამართთან მუშაობა, სამაგიეროდ დომენური სახელი ადვილად დასამახსოვრებელია, განსაკუთრებით თუ მხედველობაში მივიღებთ რომ, როგორც წესი ეს სახელი შინაარსის მატარებელია. მაგალითად, *Microsoft* კომპანიის *Web*-სერვერის სახელია www.microsoft.com, ხოლო www.internet.ge დომენი *ge*

მიუთითებს იმაზე, რომ სერვერი ეკუთვნის ინტერნეტის საქართველოს სექტორს.

მეორე მხრივ, ქსელის სერვერების ავტომატური მუშაობა ორგანიზებულია ოთხნიშნა რიცხვითი მისამართის გამოყენებით. მისი საშუალებით შუალედური სერვერები ასრულებენ სათანადო მიმართულებით მოთხოვნებისა და პასუხების გადაგზავნას ისე, რომ უცნობია თუ სად იმყოფება კონკრეტულად გამგზავნი ან მიმღები. ამიტომ აუცილებელია დომენური სახელების გადაყვანა მათთან დაკავშირებულ IP-მისამართებში. ამ საქმეს ემსახურებიან სერვერის დომენის სახელების სამსახურები DNS. ჩვენი მოთხოვნა www.pcworld.com გვერდის მიღებაზე ჯერ დამუშავდება DNS-სერვერში, ხოლო შემდეგ ის მიემართება IP-მისამართით და არა დომენის სახელით.

ფაილების გადაცემის სამსახური (FTP). ფაილების მიღება და გადაცემა ინტერნეტის სხვა სამსახურებთან შედარებით მნიშვნელოვან პროცენტს შეადგენს. ფაილის გადაცემის აუცილებლობა წარმოიშობა მაგალითად პროგრამის ფაილების მიღებისას, დიდი მოცულობის დოკუმენტების გადაგზავნისას, აგრეთვე არქივების გადაცემისას, რომლებშიც დიდი მოცულობის ინფორმაციაა თავმოყრილი.

FTP - სამსახურს (*File Translate Protocol*-ფაილების გადაგზავნის პროტოკოლი) აქვს თავისი სერვერები საერთაშორისო ქსელში, რომლებშიც ინახება მონაცემების არქივი. კლიენტის მხრიდან FTP-სერვერთან სამუშაოდ შეიძლება დაყენებული იყოს სპეციალური პროგრამული უზრუნველყოფა, თუმცა უმეტეს შემთხვევაში www ბრაუზერებს აქვთ ჩართული საშუალებები, რომლებიც ასრულებენ FTP-პროტოკოლის

უმარტივეს ოპერაციებს, მაგალითად ფაილების ჩატვირთვას სერვერებიდან.

FTP პროტოკოლი მუშაობს ერთდროულად ორ TCP-შეერთებასთან სერვერსა და კლიენტს შორის. ერთი შეერთებით ხდება მონაცემების გადაცემა, ხოლო მეორე შეერთება გამოიყენება, როგორც მმართველი. FTP პროტოკოლი ასევე წარუდგენს სერვერს იმ კლიენტის იდენტიფიკაციის საშუალებებს, რომელმაც სერვერს მიმართა. ამით ხშირად სარგებლობენ კომერციული სერვერები და შეზღუდული შეღწევის სერვერები, რომლებიც ინფორმაციას მხოლოდ რეგისტრირებულ კლიენტებს აწვდიან, ისინი მოითხოვენ მომხმარებლის სახელისა და მასთან დაკავშირებული პაროლის მითითებას. მაგრამ, ამას გარდა, არსებობენ ათი ათასობით FTP-სერვერები ყველა მსურველისათვის ანონიმური მიმართვით. ამ შემთხვევაში მომხმარებლის სახელის მაგიერ უთითებენ სიტყვას *anonymous*, ხოლო პაროლის ნაცვლად ელექტრონული ფოსტის მისამართს. უმეტეს შემთხვევაში FTP-ის პროგრამა-კლიენტები ამას ავტომატურად აკეთებენ.

IRC - სამსახური. სამსახური IRC (*Internet Relay Chat*) განკუთვნილია რამოდენიმე ადამიანის პირდაპირი დაკავშირებისათვის რეალურ დროში. ზოგჯერ IRC-სამსახურს *ჩატ-კომფერენციებს* ან უბრალოდ *ჩატს* (ლაყობობა) უწოდებენ. ტელეკომფერენციის სისტემებისაგან განსხვავებით, რომელშიც მონაწილეებს შორის კავშირი თემის განხილვისას ღია მთელი სამყაროსათვის, IRC-სისტემაში კავშირი სრულდება მხოლოდ ერთ არხში, რომლის მუშაობაში მხოლოდ რამოდენიმე ადამიანი იღებს მონაწილეობას. თვითოეულ მომხმარებელს შეუძლია შექმნას

საკუთარი არხი და მოიწვიოს მასში „საუბრის“ მონაწილეები ან შეუერთდეს მოცემულ მომენტში ერთერთ რომელიმე ღია არხს.

არსებობენ რამოდენიმე პოპულარული პროგრამა-კლიენტები იმ სერვერებსა და ქსელებთან სამუშაოდ, რომლებიც თავაზობენ IRC-სამსახურს. ასეთ ერთ ერთ პოპულარულ პროგრამას წარმოადგენს Mirc.exe

ICQ - სამსახური ეს სამსახური განკუთვნილია იმ ადამიანის IP მისამართის მოსაძებნად, რომელიც მოცემულ მომენტში მიერთებულია ინტერნეტთან. მსგავსი სამსახურის არსებობის აუცილებლობა დაკავშირებულია იმასთან, რომ მრავალ მომხმარებელს არა აქვთ მუდმივი IP-მისამართი. სამსახურის დასახელება არის გამოთქმის *I seek you-მე შენ გეძებ* აკრონიმი. ამ სამსახურით სარგებლობისათვის საჭიროა დარეგისტრირება მის ცენტრალურ სერვერზე (<http://www.icq.com>) და პერსონალური საიდენტიფიკაციო ნომერის UIN (*Universal Internet Number*) მიღება. ეს ნომერი შეიძლება აცნობოთ თქვენს პარტნიორებს კავშირში და მაშინ ICQ სამსახური იძენს ინტერნეტ-პეიჯერის ხასიათს. იცით რა პარტნიორის UIN ნომერი, მაგრამ არ იცით მისი მიმდინარე IP-მისამართი, შესაძლებელია ICQ სამსახურის ცენტრალური სერვერის საშუალებით გაუგზავნოთ მას შეტყობინება დაკავშირების წინადადებით.

როგორც ზემოთ იყო ნათქვამი ინტერნეტთან მიერთებულ თვითოეულ კომპიუტერს უნდა ქონდეს ოთხნიშნა IP-მისამართი. ეს მისამართი შეიძლება იყოს მუდმივი ან დინამიური (დროებითი). ის კომპიუტერები, რომლებიც მიერთებულია ქსელში მუდმივად აქვთ მუდმივი IP-მისამართი. მრავალი მომხმარებელი კი მიერთებულია ინტერნეტთან სეანსის განმავლობაში. მათ ეძლევათ დინამიური IP-

მისამართი, რომელიც ძალაშია მხოლოდ სენსის განმავლობაში. ამ მისამართს იძლევა ის სერვერი, რომლის საშუალებითაც ხდება დაკავშირება. სხვადასხვა სენსების დროს დინამიური IP-მისამართი შეიძლება იყოს განსხვავებული, ამასთან იგი წინასწარ უცნობია.

ინტერნეტთან ყოველი მიერთების დროს თქვენს კომპიუტერზე დაყენებული ICQ-პროგრამა განსაზღვრავს IP-მისამართს და აცნობებს ცენტრალურ სამსახურს, რომელიც, თავის მხრივ აცნობებს მას თქვენს საკონტაქტო პარტნიორებს, შემდეგ თქვენ პარტნიორებს (თუ ისინიც არიან აგრეთვე მოცემული სამსახურის კლიენტები) შეუძლიათ დაამყარონ პირდაპირი კავშირი თქვენთან. პროგრამა იძლევა რეჟიმის ამორჩევის საშუალებას („მზადა ვარ კონტაქტისათვის“, გთხოვთ არ შემაწუხოთ, მაგრამ მზად ვარ მივიღო სასწრაფო შეტყობინება“ და ა.შ). კონტაქტის დამყარების შემდეგ კავშირი სრულდება IRC სერვერის ანალოგიურ რეჟიმში.

1.6 ინტერნეტთან შეერთება.

ინტერნეტში სამუშაოდ აუცილებელია:

- ✓ ფიზიკურად მიუერთოთ კომპიუტერი საერთაშორისო ქსელის ერთ ერთ რომელიმე კვანძს.
- ✓ მიიღოთ მუდმივი ან დროებითი IP-მისამართი.

დააყენოთ და გამართოთ ინტერნეტის იმ სამსახურების პროგრამული უზრუნველყოფა - პროგრამა-კლიენტები, რომლის მომსახურებითაც აპირებთ ისარგებლოთ.

ორგანიზაციებს, რომლებიც გთავაზობენ თავის კვანძთან მიერთების შესაძლებლობას და გიყოფენ IP-მისამართს,

ინტერნეტის მომსახურების მომწოდებლებს – სერვის პროვაიდერებს უწოდებენ. მსგავს მომსახურებას სერვის პროვაიდერები ასორციელებენ ხელშეკრულების საფუძველზე.

ფიზიკური მიერთება შეიძლება იყოს *გამოყოფილი* ან *კომპუტირებული*. გამოყოფილი მიერთებისათვის აუცილებელია ან ახალი ხაზის გაყვანა ან მზა ფიზიკური კავშირის ხაზის დაქირავება (საკაბელო, ოპტიკური, რადიო არხი, თანამგზავრის არხი და ა.შ). ასეთ მიერთებას იყენებენ ის ორგანიზაციები ან საწარმოები, რომლებსაც ესაჭიროებათ დიდი მოცულობის მონაცემების გადაცემა. კავშირის ხაზის ტიპზეა დამოკიდებული მისი გამტარიანობა (იზომება ერთეულებში *ბიტ/წამში*). ამჟამად მძლავრი კავშირის ხაზების გამტარიანობა (ოპტიკური და თანამგზავრული) შეადგენს ასეულ მეგაბაიტს წამში.

სატელეფონო (კომპუტირებული) ხაზებით კავშირისათვის დამახასიათებელია დაბალი გამტარიანობა. იმის მიხედვით თუ როგორი მოწყობილობა გამოიყენება სიგნალის გაცვლისათვის ავტომატურ სატელეფონო სადგურებში, განასხვავებენ ანალოგიურ და ციფრულ სატელეფონო ხაზებს. სატელეფონო ხაზების ძირითად ნაწილს ყოფილი საბჭოთა კავშირის რესპუბლიკების ქალაქებში შეადგენს ძირითადად მოძველებული ანალოგიური ხაზები. მათი ზღვრული გამტარიანობა 31 კბიტ/წმ-ზე ცოტა მეტია (ტექსტის ერთი-ორი გვერდი ან სტანდარტული ზომის ერთი-ორი ფოტოსურათი წამში). ციფრული სატელეფონო ხაზების გამტარიანობა შეადგენს 60-120 კბიტ/წმ-ში, რაც 2-4 ჯერ მაღალია. ანალოგიური სატელეფონო ხაზებით შეიძლება ვიდეოინფორმაციის გადაცემაც (რაც გამოიყენება ვიდეოკომფერენციებში), მაგრამ ფანჯრის ზომა, რომელშიც აისახება

ვიდეომონაცემები ჩვეულებრივად მცირეა და მცირეა კადრების ცვლის სიხშირეც ხარისხიანი ვიდეოფირის მისაღებად (1-2 კადრი წამში). შედარებისათვის ჩვეულებრივი ტელეხედვის კადრების სიხშირე - 25 კადრია წამში. კავშირის სატელეფონო ხაზები არასოდეს არ იყო განკუთვნილი ციფრული სიგნალების გადასაცემად. მათი მახასიათებლები მხოლოდ ხმების გადაცემისათვისაა ვარგისი. ამასთან სიხშირის საკმაოდ ვიწრო - 3000 ჰერცი დიაპაზონში. ამიტომ ბგერითი სიხშირის სიგნალების მატარებელი ციფრული ინფორმაციის გადაცემისათვის მათ გარდაქმნიან (მოდულაცია) ამპლიტუდსა, ფაზასა და დროში. ასეთ გარდაქმნას სპეციალური მოწყობილობა - მოდემი ასრულებს (სახელწოდება მოდემი წარმოქმნილია სიტყვებისაგან მოდულატორი და დემოდულატორი).

მოდემის დაყენება.

მიერთების წესების მიხედვით განასხვავებენ გარე და შიდა მოდემებს. გარე მოდემს აერთებენ სისტემური ბლოკის უკანა მხარეს გამოტანილ მიმდევრობითი პორტის ჩამრთველში. შიდა მოდემს კი აყენებენ დედა (Mother board) პლატის გამაფართოებლის ერთ-ერთ ჩამრთველში.

მოდემში გამავალი მონაცემების ნაკადი გაცილებით მცირეა ვიდრე კომპიუტერის სხვა მოწყობილობებში გამავალი ნაკადები. ამიტომ ბოლო დრომდე მოდემებს უერთებდნენ მოძველებულ, მცირე წარმადობის მქონე სალტების ISA (Industry Standart Architecture) ჩამრთველებს (სლოტებს). ამჟამად იწარმოება მოდემები, რომელთა მიერთება გათვლილია PCI (Peripheral Control Interface) სალტებზე.

როგორც კომპიუტერის სხვა მოწყობილობები, მოდემიც საჭიროებს არა მარტო აპარატულ დაყენებას არამედ პროგრამულ გამართვასაც. ოპერაციულ სისტემაში Windows იგი შეიძლება შეკასრულით სტანდარტული საშუალებებით. Start ▶ Setting ▶ Control ▶ Panel ▶ Add Hardware. თუმცა მოდემისათვის არის სპეციალური პროგრამული საშუალება Start ▶ Setting ▶ Control ▶ Panel ▶ Phone And Modem.

PCI სალტესთან მიერთებულ მოდემისათვის დაყენების პრობლემა არ წარმოიქმნება, რადგანაც ისინი შეესაბამებიან *თვითდაყენებადი* მოწყობილობების (*plug-and-play*) სტანდარტს. ISA სალტესთან მიერთებული მოდემები ყოველთვის არ არიან თვითდაყენებადი (ისევე, როგორც ამ სალტესთან მიერთებული კომპიუტერის სხვა მოწყობილობები) და ოპერაციულმა სისტემამ შეიძლება არაკორექტულად შეასრულოს ავტომატური პროგრამული დაყენება და გამართვა. თუ ამასთან ერთად, წარმოიშვება აპარატული კომფლიქტი, მათ ხშირად მიყვევართ მოდემისა და მაუსის არასწორ მუშაობასთან. კომფლიქტის აღმოსაფხვრელად მოდემისა და მაუსის მიმდევრობით პორტებს უცვლიან დანიშნულებას და ხელახლა ასრულებენ დაყენებას.

სერვის-პროვაიდერის კომპიუტერთან დაკავშირება.

სერვის-პროვაიდერის ანუ ინტერნეტის მომსახურების მომწოდებლის კომპიუტერთან დასაკავშირებლად საჭიროა სწორად გავმართოთ ქსელთან დაშორებული შედწვევის პარამეტრები (Deal-Up Setting). პროგრამის გამართვისას აუცილებელი მონაცემები, რომელიც პროვაიდერმა უნდა მოგაწოდოთ შემდეგია:

- ✓ ტელეფონის ნომერი რომლითაც ხდება დაკავშირება;
- ✓ მომხმარებლის სახელი (Login)

- ✓ პაროლი (password)
- ✓ DNS-სერვერის IP-მისამართი (ყოველ შემთხვევაში შეაქვთ ორი მისამართი: ძირითადი და დამეტებითი, რომელიც გამოიყენება თუ რაიმე მიზეზით ძირითადი DNS-სერვერი დროებით არ მუშაობს).

ეს მონაცემები საკმარისია ინტერნეტთან მისაერთებლად, თუმცა პროვაიდერთან ხელშეკრულების დადებისას შეიძლება დამატებითი ინფორმაციის მიღება, მაგალითად, სამსახურის ტელეფონების ნომრები. პროგრამის გასამართავად საკუთარი IP-მისამართის შეტანა საჭირო არ არის. მომსახურების მომწოდებლის სერვერი ატომატურად გამოყოფს მას მუშაობის სეანსის განმავლობაში.

თავი 2. ინფორმაციის მიღება ინტერნეტიდან.

2.1 *World Wide Web – ძირითადი ცნებები*

ინტერნეტი გამოიყენება, როგორც ცოდნის სხვადასხვა სფეროებში მრავალმხრივი ინფორმაციის მიღების წყარო. დოკუმენტების უმრავლესობას, რომელიც ხელმისაწვდომია ინტერნეტის სხვადასხვა სერვერებზე, ჰიპერტექსტური ფორმატი აქვთ. ინტერნეტის სამსახურს, რომელიც მართავს ასეთი დოკუმენტების გადაცემას *World Wide Web (Web, WWW)* – მსოფლიო აბლაბუდას უწოდებენ. ამავე ტერმინით ან *WWW* გარემოთი იწოდება *Web*-დოკუმენტების ერთობლიობა, რომელთა შორის არსებობს ჰიპერტექსტური კავშირი.

WWW გარემოს არა აქვს ცენტრალიზებული სტრუქტურა. იგი ივსება მათ მიერ, ვისაც სურს განათავსოს ინტერნეტში თავისი მასალები და შეიძლება განიხილოს როგორც ინფორმაციული სივრცე. როგორც წესი *WWW*-დოკუმენტები ინახება ინტერნეტთან მუდმივად მიერთებულ კომპიუტერზე – *Web* სერვერზე. ჩვეულებრივად, *Web*-სერვერზე განათავსებენ არა ცალკეულ დოკუმენტებს, არამედ ურთიერთდაკავშირებულ დოკუმენტების ჯგუფს. ასეთი ჯგუფი წარმოადგენს *Web* კვანძს. *Web*-კვანძებზე მომზადებული დოკუმენტების განთავსებას *Web*-გამომცემლობას ან *Web* – პუბლიკაციებს უწოდებენ.

Web-არხები. ჩვეულებრივი *Web*-კვანძი ინფორმაციას მხოლოდ კლიენტის მიმართვის პასუხად გასცემს. თვალყური რომ ადევნოს გამოქვეყნებული მასალების განახლებას, მომხმარებელი

იძულებულია რეგულარულად მიაკითხოს მოცემულ კვანძს. *Web*-კვანძის თანამედროვე მოდელი საშუალებას იძლევა მოცემულ დროში გადასცეს განახლებული ინფორმაცია რევისტრირებული კლიენტის კომპიუტერზე. ისეთ *Web*-კვანძებს, რომლებსაც უნარი აქვთ დამოუკიდებლად შეასრულონ ინფორმაციის მიწოდება - არსებს უწოდებენ. არსების კონცეფციის მხარდაჭერას ახორციელებს ოპერაციული სისტემა *Windows*. კერძოდ, მასზეა დაფუძნებული სამუშაო მაგიდის - *Active Desktop* დინამიური განახლება.

Web – გვერდი. *World Wide Web*-ის ცალკეულ დოკუმენტს *Web*-გვერდებს უწოდებენ (*Web Site*). ჩვეულებრიდად იგი არის კომბინირებული დოკუმენტი, რომელიც შეიძლება შეიცავდეს ტექსტს, გრაფიკულ ილუსტრაციებს, მულტიმედიაურ და სხვა ჩართულ ობიექტებს. *Web*-გვერდის შესაქმნელად გამოიყენება *HTML (Hyper Text Markup Language)* – ჰიპერტექსტის მონიშვნის ენა, რომელიც დოკუმენტში ჩართული ტეგების - სპეციალური ნიშნების საშუალებით აღწერენ დოკუმენტის ლოგიკურ სტრუქტურას, მართავენ ტექსტის დაფორმატებას და ჩართული ობიექტების განლაგებას. ინტერაქტიული *Web*-კვანძები მომხმარებლისაგან ინფორმაციას იღებენ ფორმებით და ახდენენ მოთხოვნილი *Web* გვერდის გენერაციას სპეციალური პროგრამების (სცენარი *CGI*), დინამიური *HTML* და სხვა საშუალებებით.

ჰიპერტექსტური მიმართულები. *World Wide Web* გარემოს განმასხვავებელ თავისებურებებს წარმოადგენენ, ყოველგვარი მისამართის მითითების გარეშე, ერთი დოკუმენტიდან, მასთან თემატურად დაკავშირებულ მეორე დოკუმენტზე გადასვლის

საშუალებების არსებობა. დოკუმენტებს შორის კავშირი ხორციელდება ჰიპერტექსტური მიმართვების (ან უბრალოდ ჰიპერმიმართვების - *Hiper Link*) საშუალებით. ჰიპერმიმართვა არის დოკუმენტის გამოყოფილი ფრაგმენტი (ტექსტი ან ილუსტრაცია), რომელთანაც ასოცირებულია სხვა *Web*-დოკუმენტის მისამართი. ჰიპერმიმართვის გამოყენებისას (მასზე მაუსის მიმთითებლის მიტანა და ერთხელ დაწკაპუნება) სრულდება ჰიპერმიმართვაზე გადასვლა, ანუ იმ *Web*-გვერდის გახსნა, რომელზეც მიუთითებს მიმართვა. ჰიპერმიმართვების გამოყენება საშუალებას იძლევა *World Wide Web*-გარემოში ვაწარმოთ თემატური მოგზაურობების ორგანიზაცია კონკრეტული გვერდების მისამართების ცოდნის გარეშე.

დოკუმენტების მისამართები. ინტერნეტის დოკუმენტების მისამართების ჩასაწერად გამოიყენება ფორმა, რომელსაც *URL* მისამართს უწოდებენ (*Uniform Recourse Locator*). *URL* მისამართი შეიცავს მითითებებს პროტოკოლის, კომპიუტერის მისამართისა და ამ კომპიუტერზე დოკუმენტის მოძებნის გზის შესახებ. კომპიუტერის მისამართი შედგება რამოდენიმე, ერთმანეთისაგან წერტილებით გამოყოფილი ნაწილისაგან. მაგალითად, *www.internet.ge*. მისამართის ელემენტები, განლაგებული მარჯვნივ, განსაზღვრავენ კომპიუტერის მიკუთვნებას ქსელისადმი, ხოლო მარცხენა ელემენტები მიუთითებენ მოცემული ქსელის კონკრეტულ კომპიუტერზე. *URL* მისამართის *IP*-მისამართის ციფრულ ფორმაში გარდაქმნას აწარმოებს დომენების სახელების სამსახური (*Domain Name Service, DNS*). ინტერნეტის დოკუმენტის მოძებნის გზაში განმამხოლოებელ ნიშნად გამოიყენება დახრილი ხაზი „/“.

ინტერნეტის გვერდების დათვალიერების საშუალებები.

ინტერნეტის დოკუმენტები განკუთვნილია ელექტრონულ ფორმაში გამოსასახავად, ამასთან დოკუმენტის ავტორისათვის უცნობია იმ კომპიუტერის შესაძლებლობები, რომელზეც აისახება დოკუმენტი. ამიტომ, ენა *HTML* უზრუნველყოფს არა იმდენად დოკუმენტის ფორმატირებას, არამედ მისი ლოგიკური სტრუქტურის აღწერას. დოკუმენტის ფორმატირება და გამოსახვა კომპიუტერებზე სრულდება სპეციალური პროგრამით ბრაუზერით (*Browser*).

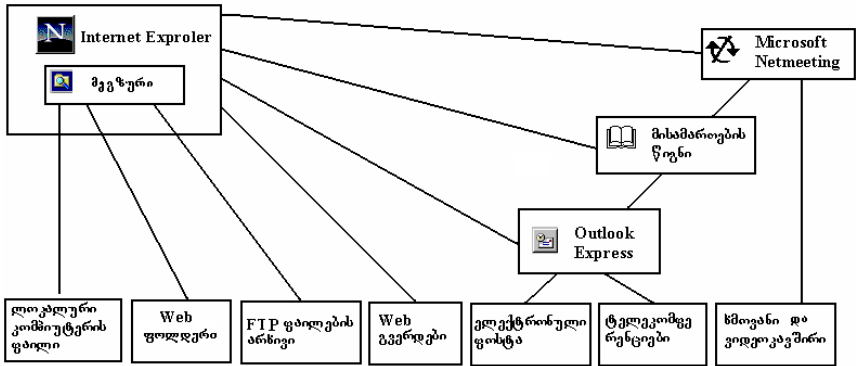
ბრაუზერის ძირითადი ფუნქციებია:

- ✓ Web - სერვერთან კავშირის დამყარება, რომელზეც ინახება დოკუმენტი და კომბინურებული დოკუმენტის ყველა კომპონენტების ჩატვირთვა;
- ✓ HTML ენის ტეგების ინტერპრეტაცია, Web - გვერდის ფორმატირება და ასახვა იმ კომპიუტერის შესაძლებლობების შესაბამისად, რომელზეც მუშაობს ბრაუზერი;
- ✓ Web - გვერდში შემავალი მულტიმედიის და სხვა ობიექტების ასახვის საშუალებების მიწოდება, აგრეთვე იმ საშუალებების მიწოდება, რომელიც მომართავს პროგრამას ახალი ტიპის ობიექტთან სამუშაოდ;
- ✓ Web - გვერდის მოძებნის ავტომატიზაციის უზრუნველყოფა და იმ Web - გვერდებთან მიღწევის გამარტივება, რომლებთანაც ადრეც იყო მიმართვები;
- ✓ ინტერნეტის სხვა სამსახურებთან სამუშაოდ შესაბამისი საშუალებების მიწოდება.

2.2 *Internet Explorer პროგრამასთან მუშაობა.*

ინტერნეტის მხრიდან WWW სამსახურის მუშაობას უზრუნველყოფენ სერვერული პროგრამები, Web სერვერები. მომხმარებლის მხრიდან მუშაობას უზრუნველყოფს კლიენტის პროგრამები, Web - ბრაუზერები. უფრო მეტად ცნობილი ბრაუზერებია: *Internet Explorer* (კომპანია *Microsoft*), *Netscape Navigator* (კომპანია *Netscape Communications*) და *Opera* (კომპანია *Opera Software*). პრინციპში, ყველა ბრაუზერები ერთი და იგივე ფუნქციებს ასრულებენ, ხოლო ამა თუ იმ კონკრეტული ბრაუზერის ამორჩევა გემოვნებისა და ჩვევების საქმეა. მაგრამ, ბრაუზერს *Microsoft Internet Explorer* (ინტერნეტის მეგზური) ყველა სხვა დანარჩენებთან ის უპირატესობა აქვს, რომ იგი შედის ოპერაციული სისტემის შემადგენლობაში და წარმოადგენს მის განუყოფელ კომპონენტს.

Windows 98 ოპერაციული სისტემის ბოლო ვერსიიდან მოყოლებული მომხმარებელს მიეწოდება ბრაუზერის *Internet Explorer 5.0* და შემდგომი ვერსიები. პროგრამა უზრუნველყოფს კომპიუტერის ლოკალურ დოკუმენტებთან, კორპორაციული ქსელის - *Internet* რესურსებთან და ინტერნეტით ხელმისაწვდომ ინფორმაციასთან შედწევის ერთიან მეთოდს. იგი უზრუნველყოფს *World Wide Web* ის მუშაობას, გვაძლევს კომპიუტერის ლოკალურ საქაღალდეებთან (*Folder*) და *FTP* ფაილების არქივებთან მუშაობის იდენტურ საშუალებებს. პროგრამები (*Outlook Express* და *Microsoft Netmeeting*) ავტონომიურია, მაგრამ განიხილებიან, როგორც *Internet Explorer* პაკეტის ნაწილი. *Internet Explorer* საშუალებით ინტერნეტის გამოყენების სქემა მოცემულია ნახაზზე 1.



ნახ 1 ინტერნეტის რესურსებთან შეღწევის ორგანიზაცია

Internet Explorer ბრაუზერის გასაშვებად შეიძლება გამოვიყენოთ *Internet Explorer*-ის პიკტოგრამა სამუშაო მაგიდაზე ან სწრაფი გაშვების პანელზე. აგრეთვე მთავარი მენიუ (Start ► Program ► Internet Explorer). გარდა ამისა პროგრამა ავტომატურად ეშვება ინტერნეტის დოკუმენტის ან *HTML* ფორმატში ლოკალური დოკუმენტის გახსნის მცდელობისას. ამ მიზნით შეიძლება გამოვიყენოთ Web გვერდის იარაღი ან პუნქტი *Favorites* (რჩეული) პროგრამა *Internet Explorer*-ის მენიუს სტრიქონიდან ან შეტანის ველი დიალოგურ ფანჯარაში Start ► Run (პროგრამის გაშვება). *Internet Explorer*-ის პარამეტრების გამართვა (მომხმარებლის გარემოს დაყენება) ხორციელდება *Internet Options* დიალოგურ ფანჯარაში, რომლის გააქტიურება შესაძლებელია, როგორც *Internet Explorer*-ის მენიუდან ბრძანებით Tool ► Internet Options ისე მართვის პანელიდან Start ► Setting ► Control Panel ► Internet Options. თუ ინტერნეტთან კავშირი არაა დამყარებული შენარჩუნებულია ადრე ჩატვირთვული Web დოკუმენტების ავტონომიურ რეჟიმში დათვალიერების შესაძლებლობა. კავშირის არსებობისას, პროგ-

რამის გაშვების შემდეგ ეკრანზე გამოდის ე.წ. საწყისი გვერდი, რომელიც მითითებულია პროგრამის გამართვისას.

2.3 *Web გვერდის დათვალიერება*

დასათვალიერებელი *Web*-გვერდი აისახება ფანჯრის მუშა არეში. გაჩუმებით ეკრანზე წარმოჩნდება მთელი მისი შემადგენლობა გრაფიკული ილუსტრაციების და ჩართული მულტიმედიური ობიექტების ჩათვლით. დათვალიერების მართვა ხორციელდება მენიუს სტრიქონიდან, ინსტრუმენტის პანელიდან, აგრეთვე ღია დოკუმენტში არსებული აქტიური ელემენტების საშუალებით, კერძოდ ჰიპერმიმართვებით.

თუ *Web*-გვერდის *URL* მისამართი ცნობილია, იგი შეიტანება მისამართის - *Address* ველში და აქტიურდება ღილაკი - *Go* (გადადი). მისამართის ველში მითითებული გვერდი აისახება ეკრანზე უკვე გამოსახული გვერდის ნაცვლად. მისამართის განმეორებით შეტანას ამარტივებს სტრიქონის ავტოშევსების შესაძლებლობის არსებობა. შესატანი მისამართი ავტომატურად დარდება ადრე დათვალიერებული *Web* გვერდის მისამართებს. ყველა შესაფერისი მისამართი აისახება მისამართის ველში გახსნილ სიაში. თუ სიაში არის საჭირო მისამართი, მისი ამორჩევა ხდება კლავიშებით „ზევით“ და „ქვევით“ და მასზე დაწკაპუნებით, რის შედეგადაც დაწკაპუნდება ღილაკზე გადადი (*Go*). სიაში მისამართის არ არსებობის შემთხვევაში მისამართის შეტანა ხდება ჩვეულებრივად ხელით.

ჰიპერმიმართვებთან მუშაობა. ხშირად ინტერნეტში ნავიგაცია არა *URL* მისამართის შეტანით ხდება, არამედ ჰიპერმიმართვების გამოყენებით. *Web* გვერდის ეკრანზე გამოსახვისას

ჰიპერმიმართვები ჩვეულებრივად ლურჯით ფერით ან ხაზგასმით გამოირჩევიან. ჩვეულებრივად ხაზგასმა გამოიყენება მხოლოდ ჰიპერმიმართვების გამოსაყოფად. უფრო საიმედო ნიშანს წარმოადგენს მაუსის მიმთითებლის ფორმა. ჰიპერმიმართვაზე მოხვედრისას ის იღებს ხელის მტევნის ფორმას, ხოლო თვითონ ჰიპერმიმართვა, ბრაუზერის შესაბამისი გამართვისას იცვლის ფერს. *URL* მისამართი, რომელზედაც მიუთითებს მიმართვა, აისახება მდგომარეობის სტრიქონში. ჰიპერმიმართვაზე დაწკაპუნებისას, ჩაიტვირთება შესაბამისი *Web*-გვერდი მიმდინარის ნაცვლად. თუ ჰიპერმიმართვა მიუთითებს ნებისმიერ ფაილს, მისი ჩაიტვირთვა ხდება *FTP* პროტოკოლით.

Web-გვერდებზე შეიძლება აგრეთვე შეგვხვდეს გრაფიკული მიმართვები ანუ ნახატებით წარმოდგენილი ჰიპერმიმართვები და გამოსახულება-ნიშნებით, რომლებიც აერთიანებენ რამოდენიმე მიმართვას ერთი გამოსახულების ჩარჩოებში. ღია *Web*-გვერდზე მიმართვების დასათვალიერებლად მოხერხებულია *Tab* კლავიშის გამოყენება. ამ კლავიშზე ხელის დაჭერისას შეეყვანის ფოკუსი (წყვეტილხაზიანი ჩარჩო) გადაადგილდება მომდევნო მიმთითებელზე. მიმთითებელზე გადასვლა შეიძლება *Enter* ღილაკზე ხელის დაჭერითაც. ასეთი მიდგომით, თანდათანობით გადაირჩევა ტექსტური და გრაფიკული მიმართვები, აგრეთვე გამოსახულება-ნიშნების ცალკეული სფეროები.

ჰიპერმიმართვების გამოყენების დამატებით საშუალებებს იძლევა მათი კონტექსტური მენიუ. ახალი გვერდის გასახსნელად ძველის დახურვის გარეშე იყენებენ ბრძანებას *Open New Window* (გახსენი ახალ ფანჯარაში). შედეგად გაიხსნება ბრაუზერის ახალი ფანჯარა. *URL* მიმართვით მითითებული მისამართი

შეიძლება მოვათავსოთ გაცვლის ბუფერში (*Clipboard*) ბრძანებით – *Create Shortcut* (იარლიყის ასლი). იგი შეიძლება ჩაესვათ მისამართის ველში (*Adress*) ან სხვა ნებისმიერ დოკუმენტში შემდგომი გამოყენების მიზნით.

ასევე მოხერხებულია კონტექსტური მენიუს გამოყენება მიმდინარე გვერდსა და მის ელემენტებზე სხვა ოპერაციების განსახორციელებლად. ასე მაგალითად, გვერდზე მოთავსებული სურათი შეიძლება:

- ✓ შევინახოთ, როგორც ფაილი (*Save Picture As*);
- ✓ გამოვიყენოთ, როგორც ფონური სურათი (გახსადოთ, როგორც სამუშაო მაგიდის სურათი) ან როგორც აქტიური ელემენტი (შევინახოთ, როგორც სამუშაო მაგიდის ელემენტი).

თუ ნახატი ასრულებს გრაფიკული მიმართვის ფუნქციებს, მასზე შეიძლება გამოვიყენოთ ბრძანებები, რომლებიც ხეობიან როგორც გამოსახულებას, ასევე მიმართვებს.

2.4 ბრაუზერის მართვის მეთოდები.

WWW დოკუმენტების დათვალიერების დროს გარკვეული მოქმედებების აუცილებლობა თვით მუშაობის მსველელობითაა ნაკარნახევი. ასეთ შემთხვევებში მოხერხებულია ინსტრუმენტების პანელის ღილაკების, (*Standard Buttons*) გამოყენება. იმისათვის, რომ დავუბრუნდეთ რამოდენიმე ხნის წინ დათვალიერებულ გვერდს, გამოვიყენება ღილაკი „*Back*“ (უკან). რამოდენიმე გვერდით უკან დასაბრუნებლად შეიძლება, აგრეთვე გამოვიყენოთ მასთან დაკავშირებული ჩამოსაშლელი სიის ღილაკი. შესრულებული მოქმედების გასაუქმებლად გამოვიყენება ღილაკი *Forward* (წინ). თუ გვერდის ჩატვირთვის პროცესი გაჭიანურდა ან აღარაა აუცილე-

ბელი, იყენებენ ღილაკს *Stop* (შეჩერდი). *Web* გვერდის ხელახლა ჩატვირთვა, თუ მისი ჩატვირთვა შეწყდა ან დოკუმენტის შინაარსი შეიცვალა, სრულდება ღილაკით *Update* (განახლება). საწყისი გვერდის დაუყონებლივ ჩატვირთვისათვის, რომლითაც ჩვეულებრივად ბრაუზერი იწყებს მუშაობას, იყენებენ ღილაკს *home* (საწყისი გვერდი).

ახალი ფანჯრის შექმნა, გახსნილი დოკუმენტის შენახვა კომპიუტერზე, დაბეჭვდა, ავტონომიური რეჟიმის ჩართვა/გამორთვა, აგრეთვე პროგრამასთან მუშაობის დამთავრება სრულდება *File* მენიუს ბრძანებებით.

გაცვლის ბუფერში დოკუმენტის ფრაგმენტების ასლის შენახვა და *Web* გვერდზე ტექსტის ძებნა სრულდება *Edit* მენიუს ბრძანებებით.

ფანჯრის მომსახურე ელემენტების გამოტანის ჩართვა და გამორთვა (ინსტრუმენტების პანელი, დამატებითი პანელები, მდგომარეობის სტრიქონი), სიმბოლოების შრიფტისა და კოდირების შერჩევა, სრულდება *View* მენიუს ბრძანებებით.

რეგულარულად დასათვალიერებელი გვერდების სიის წარმოება და მათთან სწრაფი შედღვევა ხორციელდება მენიუს *Favorite* ბრძანებებით. ინტერნეტის სხვა სამსახურებთან სამუშაო პროგრამების გამოყენებაზე გადასვლა, აგრეთვე ბრაუზერის გამართვა (პარამეტრების და რეჟიმების გამართვა) ხორციელდება მენიუს *Tools* შესაბამისი ბრძანებებით.

რამოდენიმე ფანჯარასთან მუშაობა, არც თუ იშვიათად წარმოიქმნება ახალი *Web* დოკუმენტის გახსნის აუცილებლობა მიმდინარე დოკუმენტის დაუსურავად. მაგალითად, იმ შემთხვევებში, როდესაც მიმდინარე დოკუმენტი შეიცავს საინტერესო

მიმოთიებლებს. *Internet Explorer* პროგრამის ახალი ფანჯარის გასახსნელად იყენებენ ბრძანებას *File ▶ New Window*. თვითოეული ფანჯარა ასახავს თავის *Web* დოკუმენტს და შეიძლება გამოყენებული იქნას დამოუკიდებლად. კერძოდ, ლიდაკებით *Back* და *Forward* სიები თვითოეულ ფანჯარაში ინდივიდუალურად განახლდება.

Internet Explorer პროგრამის ფანჯრების დახურვა შეიძლება ნებისმიერი თანმიმდევრობით და არა მხოლოდ იმ თანმიმდევრობით, რომლითაც ისინი გაიხსნა. მაგრამ, ბოლო ფანჯრის დახურვისას კომპიუტერზე, შეიძლება აღარ დარჩეს ღია პროგრამები, რომლებიც გამოიყენება ინტერნეტის მიერ. ამ შემთხვევაში ეკრანზე გამოიტანება გამაფრთხილებელი შეტყობინება, რომელიც თუკი კავშირი სინამდვილეში საჭირო აღარ არის შეერთების გათიშვის (*Disconnect*) შესაძლებლობას იძლევა.

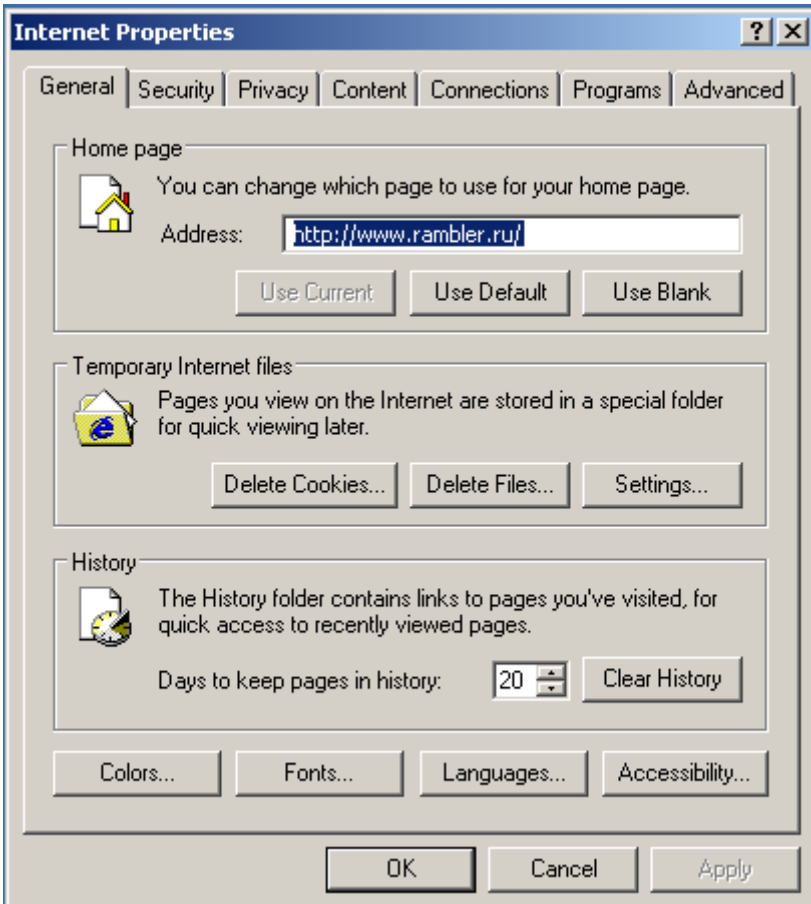
ბრაუზერის პარამეტრების გამართვა. ინტერნეტში კომფორტული და ეფექტური მუშაობისათვის აუცილებელია ბრაუზერის პარამეტრების გამართვა. ოპტიმალური გამართვის პარამეტრები დამოკიდებულია მრავალ ფაქტორზე:

- ✓ კომპიუტერის ვიდეოსისტემის პარამეტრები;
- ✓ ინტერნეტთან მოქმედი შერთების წარმადობა;
- ✓ მიმდინარე *Web* დოკუმენტის შემადგენლობა;
- ✓ ინდივიდუალური მომხმარებლის პირადი უპირატესობები.

Internet Explorer პროგრამის გამართვა შეიძლება დავიწყოთ, როგორც თვით ამ პროგრამიდან *Tools ▶ Internet Options*, ასევე ზოგად სისტემური მენიუდან *Start ▶ Setting ▶ Control Panel ▶ Internet Options* გასხნილი დაილოგური ფანჯარა ამ შემთხვევაში

მხოლოდ სახელით განსხვავდება (*Internet Options* და *Internet Property*). სხვადასხვა პარამეტრების ჯგუფის გასამართავად იგი შეიცავს 6 ჩანართს (სურათი 2). ბრაუზერის მუშაობის საერთო პარამეტრებს აყენებენ ჩანართიდან საერთო (*General*). აქ შეიძლება მიეუთითოთ, რომელი გვერდი გამოვიყენოთ როგორც საწყისი ჩატვირთვის გვერდი, მიეუთითოთ დისკური სივრცის მოცულობა ინტერნეტიდან მიღებული დროებითი ფაილების შესანახად, დროებითი ფაილების წაშლა, აგრეთვე გვერდები, რომლებიც მომზადებული იყო ავტონომიურ რეჟიმში წასაკითხად. დროებითი ფაილების შენახვის წესის მითითება ხდება დილაკით *Setting* (პარამეტრები). რაც უფრო იშვიათად ამოწმებს პროგრამა ადრე ჩატვირთული გვერდის და რეალური დოკუმენტის ვერსიის შესაბამისობას, მით მეტია გვერდის ჩატვირთვის დროის ეკონომია, მაგრამ იზრდება მათი მოძველების რისკი. სტანდარტული ინსტრუმენტების პანელზე მოთავსებული დილაკი *Update* იძლევა დოკუმენტის ყველაზე ბოლო ვერსიის მიღების საშუალებას.

გამოსასახი *Web*-გვერდების გაფორმების მართვაც სრულდება ჩანართის *General* მართვის ელემენტებით. გამოსაყენებელი ფერების დაყენება ხდება დილაკით *Color*, ხოლო შრიფტებისა – დილაკით *Font*. ეს პარამეტრები ექვემდებარებიან თვით *Web*-დოკუმენტში მითითებულ პარამეტრებს.



სურ. 2 Web-ვებრის გამოსახვის ძირითადი პარამეტრების გამართვის მართვა.

ინტერნეტთან შეერთების პარამეტრების გამართვა სრულდება ჩანართიდან *Connect*. აქ ხელმისაწვდომია იგივე ოპერაციები, რაც უშუალოდ ქსელთან დაშორებული შედგენის საქადალდის (*Network Connections*) უშუალო გამოყენებისას. გარდა ამისა შეიძლება მიეუთითოთ, თუ ზუსტად რომელი შეერთება გამოიყენება ბრაუზერის მუშაობის დროს. გადამრთველების

საშუალებით შეიძლება მიეთითოს უარი ავტომატური შეერთების გამოყენებაზე და სხვა.

ინტერნეტში სამუშაოდ პროგრამების ამორჩევა სრულდება ჩანართიდან - *Programm*. ყველა სახის პროგრამები, გარდა კალენდარისა, (საქმეთა წარმოების, შეხვედრების, დღესასწაულების და სხვა) შედიან უშუალოდ *Internet Explorer*-ის დისტრიბუტულ პაკეტში.

Web-დოკუმენტების პოტენციალურად საშიში შემადგენლობისაგან დაცვის საშუალებას გვაძლევს ჩანართი *Cecurity* (უსაფრთხოება). იგი საშუალებას იძლევა მივუთითოთ ის *Web*-კვანძები, რომლებთანაც ურთიერთობა შეიძლება საშიშად ჩაითვალოს და აუკრძალოთ მათგან ინფორმაციის მიღება.

სხვა პარამეტრები თავმოყრილია ჩანართში *Advansed* (დამატებითი), მათი საშუალებით შესაძლებელია:

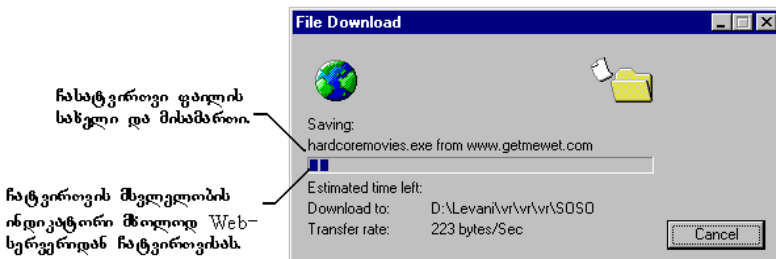
- ✓ მუშაობის კონფიდენციალობის დაცვა დაშიფრით, ელექტრონული სერთიპიკატის გამოყენებით და დროებითი ფაილების დროული განადგურებით;
- ✓ ენის – Java (ჯავა) გამოყენების კონტროლი;
- ✓ მულტიმედიის ობიექტების გამოსახვის მართვა;
- ✓ გაფორმების დამატებითი გამართვების გამოყენება;
- ✓ საჭირო ინფორმაციის შემცველი *Web*-გვერდების ძებნის რეჟიმების მართვა.

2.5 ფაილების მიღება ინტერნეტიდან

Web-გვერდზე არსებული ჰიპერმიმართებები შეიძლება მიუთითებდნენ სხვადასხვა ტიპის დოკუმენტებზე. თუ ბრაუზერს არ შეუძლია ასახოს განსაზღვრული ტიპის ფაილები (მაგალითად, პროგრამის ფაილები გაფართოებით .Exe, არქივები .Zip და სხვა) ინიცირდება მოცემული ფაილის კომპიუტერში ჩატვირთვის პროცესი.

პროგრამა *Internet Explorer* უშვებს ფაილის ჩატვირთვის ოსტატს (*Wizard*), რომლის მეშაობის პირველ ეტაპზე საჭიროა მიეთითოს უნდა გაიხსნას ფაილი თუ შეინახოს დისკზე. ფაილის „გაიხსნა“-ში იგულისხმება მისი შენახვა დროებითი ფაილების კატალოგში და დაუყონებლივი გაშვება (თუ ეს პროგრამის ფაილია) ან გაიხსნა იმ პროგრამის საშუალებით, რომელიც განკუთვნილია ამ ტიპის ფაილებთან სამუშაოდ. ასეთი მიდგომა გზას უხსნის კომპიუტერზე საფრთხის შემცველ ინფორმაციას. უფრო საიმედოა ფაილის შენახვა დისკზე. ამ შემთხვევაში საჭიროა იმ საქაღალდის ამორჩევა, რომელშიც შეინახება ფაილი და ფაილზე სახელის დარქმევა.

ფაილის ჩატვირთვის მსვლელობა აისახება სპეციალურ ფანჯარაში (სურათი 3).



სურათი 3. FTP - კვანძიდან ფაილის ჩატვირთვა.

მუშაობის მსვლელობის პროცესი გამოჩნდება მხოლოდ იმ შემთხვევაში, როდესაც ჩატვირთვის მართვის ოსტატს შეუძლია მიიღოს ინფორმაცია ფაილის სრულ მოცულობაზე, ეს კი შესაძლებელია მხოლოდ მაშინ თუ ფაილი იტვირთება უშუალოდ Web-კვინიდან.

ფაილის FTP კვინიდან ჩატვირთვის მსვლელობას შეიძლება თვალი ვადევნოთ ფანჯრის სათაურის სტრიქონით, ან თუ ფანჯარა დახურულია ან დაფარული სხვა ფანჯრებით მაშინ ამოცანების პანელზე ღილაკის წარწერით. ფაილის ჩატვირთვის პროცესი ხელს არ უშლის პარალელურად Web-გვერდის დათვალიერებას ან ინტერნეტის სხვა ოპერაციების შესრულებას. ჩატვირთვის შემდეგ ფანჯარა ავტომატურად იხურება თუ დაყენებულია ალამი - "დახურე დიალოგური ფანჯარა ჩატვირთვის დამთავრების შემდეგ". წინააღმდეგ შემთხვევაში, ჩატვირთვის დამთავრების შემდეგ გააქტიურდება ღილაკები გახსნა ან საქაღალდის გახსნა, რომლებიც საშუალებას გვაძლევენ, შესაბამისად გავხსნათ ახლახან ჩატვირთული ფაილი ან ამ ფაილს შემცველი ფოლდერი.

ფაილების ჩატვირთვა ნებისმიერ დროს შეიძლება შეწყდეს ღილაკით *Cansel*. მომხმარებლის მიერ ჩატვირთვის ან კავშირის გაწყვეტით ეს ოპერაცია საჭიროა თავიდან დაიწყოს. Windows ოპერაციულ სისტემას არა აქვს რაიმე მიზეზით შეწყვეტილი ჩატვირთვის განახლების საშუალებები. ეს შესაძლებელია მხოლოდ სპეციალური პროგრამების გამოყენებით.

ფაილები, რომლებიც მისაწვდომია ჩასატვირთად ნებისმიერი მომხმარებლისათვის, უმეტესწილად ინახებიან FTP კვინებზე. FTP კვინებზე შესაძლებელია საჭიროა მისამართის ველში მისი

URL მისამართის მითითება. გაჩუმებით (*Default*) ბრაუზერი (*Internet Explorer*) უზრუნველყოფს *FTP* - კვანძთან ანონიმურ მიერთებას, რომლის დროსაც დაშვებულია მხოლოდ ფოლდერების დათვალიერება და ფაილების ჩატვირთვა, თუ ანონიმური შეღწევა ნებადართული არ არის, ეკრანზე გამოჩნდება დიალოგური ფანჯარა სახელისა და პაროლის მოთხოვნით. *FTP*-კვანძის ფანჯარა ისევე გამოიყურება, როგორც ჩვეულებრივი საქაღალდის ფანჯარა, მაგრამ დაშორებული საქაღალდის ნიშნის გამოყენებით. ფაილის ჩასატვირთვად საჭიროა მის ნიშანზე მაუსის მარჯვენა ღილაკის დაწკაპუნება და კონტექსტურ მენიუში ასლის გადატანის ბრძანების (*Cory Folder*) ამორჩევა. თუ *FTP* პროტოკოლის მოცემული საქაღალდისათვის დაშვებულია ყველა ფაილური ოპერაციები, მაშინ მათთან შეიძლება ისევე მუშაობა, როგორც საქაღალდის ფანჯარასთან. შეუძლებელია მხოლოდ ერთი კვანძიდან მეორეზე ფაილების პირდაპირი გადატანა. ასეთი ოპერაციების შესასრულებლად საჭიროა ფაილის გადატანა ჯერ კომპიუტერის ლოკალურ საქაღალდეში, ხოლო შემდეგ ფაილის გაგზავნა აქედან სხვა *FTP* - კვანძზე ან იგივე *FTP* კვანძის სხვა საქაღალდეში. ვინაიდან შეტყობინებები შემოდიან და იგზავნიებიან სერვერის საშუალებით, პროგრამაში მოითხოვება სერვერის შესახებ ინფორმაციის მითითება. ეს ინფორმაცია ინახება საადრიცხვო ჩანაწერის სახით.

2.6 ინფორმაციის ძებნა ინტერნეტში.

ინტერნეტს სამი ფუნქცია აქვს: საკომუნიკაციო, საინფორმაციო და მართვითი. სხვადასხვა სამსახურებს შეუძლიათ უზრუნველყონ სხვადასხვა ფუნქციები. თუმცა WWW სამსახურის

ფარგლებში არიან სერვისები, რომლებიც ასრულებენ საკომუნიკაციო და მართვის ფუნქციებს, მაგრამ ამ სამსახურის ძირითადი დანიშნულება საინფორმაციოა. როდესაც გვინდა რაიმე ცნობების მოძიება, მონაცემებისათვის პირველ რიგში ვაკითხავთ *Web*-საინფორმაციო სივრცეს.

ეს სივრცე გამოირჩევა გიგანტური ზომებით, მასში წარმოდგენილია უამრავი *Web*-დოკუმენტი. მოვნახოთ მათ შორის საჭირო გვერდი განსაკუთრებული, არც თუ მარტივი ამოცანაა. რატომ უნდა, შეიძლება ვისარგებლოთ ნაცნობების რჩევით, მასიური ინფორმაციის საშუალებებში გამოქვეყნებული *URL*-მისამართებით, მაგრამ *WWW*-სამსახურისათვის აუცილებელია თავისი საძიებო სერვისები, და ისინი არსებობენ კიდევ. ეს სერვისები უფასოდ მუშაობენ. მათი საქმიანობის ეკონომიკურ საფუძველს უზრუნველყოფს კლიენტების ძალზე მაღალი უკუშვების კოეფიციენტი.

საძიებო სისტემა წარმოადგენს სპეციალიზირებულ *Web*-კვანძს. მომხმარებელი საძიებო სისტემას ატყობინებს მონაცემებს საძებნი *Web*-გვერდის შინაარსზე, ხოლო სისტემა წარუდგენს მას იმ გვერდების ჰიპერმიმართვების სიას, რომლებიც შესაბამებიან მოითხოვნას. არსებობს რამოდენიმე მოდელი, რომელზედაც დამყარებულია საძიებო სისტემების მუშაობა, მაგრამ ისტორიულად მეტი პოპულარობა ორმა მოდელმა მოიპოვა. ესენია: საძიებო კატალოგები და ძიების მიმთითებლები.

საძიებო კატალოგები. საძიებო კატალოგები აწყობილია იგვე პრინციპზე, როგორც მსხვილი ბიბლიოთეკების თემატური კატალოგები. საძიებო კატალოგებზე მიმართვისას, მის ძირითად გვერდზე ვნახულობთ მსხვილი თემატური კატეგორიების სიას,

მაგალითად ისეთი, როგორცაა ეკონომიკა და მეწარმეობა (*Business Economika*), რომელიც ნაჩვენებია საძიებო კატალოგების *yahoo!* მაგალითზე (სურ. 5).

კატალოგების სიის თვითოეული ჩანაწერი ჰიპერმომარტავა. მასზე დაწკაპუნებით იხსნება საძიებო კატალოგის შემდეგი გვერდი, რომელზეც დაწვრილებითაა წარმოდგენილი მოცემული თემა, მაგალითად, თემებზე: სამეწარმეო სამართალი, მომხმარებლის უფლებების დაცვა,



სურ. 5 საძიებო კატალოგების *yahoo!* მთავარი გვერდი

ეკონომიკური მანკებებლები და ბაზრის ინდიკატორები, რეკლამა და მარკეტინგი, ელექტრონული კომერცია და სხვა მრავალი. თემის დასახელებაზე დაწკაპუნებით (მაგ. ელექტრონული კომერცია) იხსნება ახალი გვერდი განყოფილებების სიით - ელექტრონული საგადასახადო სისტემები, ინტერნეტ-მაღაზიები, ელექტრონული კომერციის საწარმოების დაბეგერა, პროგრამული

უზრუნველყოფა და სხვა. თემაში ჩაღრმავების გაგრძელებით, შეიძლება მივაღწიოთ კონკრეტული Web-გვერდების სიასთან და ამოვირჩიოთ ის რესურსები, რომელიც უკეთ შეესაბამება ამოცანის გადაწყვეტას. საძიებო სისტემებთან მუშაობა ინტუიციურად მარტივია. მათში ინფორმაციის ძიება ცოტა თუ ბევრად პრაქტიკულად ყოველთვის ნაყოფიერად მთავრდება. თუმცა ამ სიმარტივის მიღმა კატალოგების შექმნისა და წარმოების მეტისმეტი სირთულე იმალება. მაღალკვალიფიციური რედაქტორები პირადად ათვალიერებენ WWW საინფორმაციო სივრცეს, არჩევენ იმას, რაც მათი თვალსაზრისით საზოგადოების ინტერესს წარმოადგენს და შეაქვთ მისამართები კატალოგში. მსოფლიოს უმსხვილესი საძიებო კატალოგია Yahoo! (www.yahoo.com). მას ემსახურება დაახლოებით 150 რედაქტორი, ამის მიუხედავად კატალოგიზირებული Web რესურსების საერთო მოცულობა შეადგენს მილიონ Web-გვერდზე მეტს, რაც მთელი WWW რესურსების 10%-ზე ნაკლებია.

მიუხედავად ასეთი დაბალი კოეფიციენტისა საძიებო კატალოგები დიდი პოპულარობით სარგებლობან. მიღებულია მათი გამოყენება მოცემულ თემაზე ინფორმაციის პირველადი, რეფერატული ძებნისათვის. თუ თემა მომხმარებლისათვის ახალია და გამოუკვლევია, მაშინ ის ალბათ არ საჭიროებს ძებნის ფართო შედეგებს. უმეტესად ის საჭიროებს ცოტად თუ ბევრად შინაარსიანი რესურსების მიმთითებლებს, რასაც უზრუნველყოფენ სწორედ საძიებო კატალოგები. გამომდინარე იქიდან, რომ კატალოგის შედგენაზე მუშაობენ ადამიანები და არა პროგრამები უზრუნველყოფს თვითოეულ თემაზე უფრო მნიშვნელოვანი რესურსების შერჩევას.

საძიებო კატალოგების რიცხვი მსოფლიოში შედარებით მცირეა. რაც დაკავშირებულია მათი შენახვისა და მომსახურების მაღალ შრომატევადობასთან და კვალიფიციური რედაქტორების სიმცირესთან. მსოფლიოს უმსხვილესი საძიებო კატალოგი უკვე დავასახელეთ, რუსეთის უდიდესი საძიებო კატალოგია *Atrus-ი* (*atrus.aport.ru*). ზოგიერთი თანამედროვე საძიებო კატალოგების სია მოტანილია წიგნის ბოლოში.

საძიებო მიმითებლები. საძიებო კატალოგების ძირითად პრობლემას *WWW*–რესურსების მოცვის დაბალი კოეფიციენტი წარმოადგენს. თუმცა რეფერატული ძებნისათვის იგი კრიტიკულად არ გამოიყურება, მაგრამ მაინც არსებობენ აქტუალურ, უნიკალურ, სპეციალურ ინფორმაციაზე მოთხოვნები, რომელსაც არ მოიცავს და არც შეიძლება მოიცავდეს საძიებო კატალოგები.

იმისათვის, რომ მრავალჯერ გაიზარდოს *Web*–რესურსების მოცვის კოეფიციენტი, საძიებო სისტემის მანაცემთა ბაზის შევსების პროცესიდან აუცილებელია ადამიანის ფაქტორის გამორიცხვა, სამუშაო უნდა იყოს ავტომატიზირებული, ამასთან ერთად მნიშვნელოვნად ეცემა სისტემის მიერ ძიების შედეგად მოწოდებული მიმართვების ხარისხი, მაგრამ იმავდროულად იზრდება მათი რაოდენობა. *Web*–რესურსების ავტომატურ კატალოგიზაციას და კლიენტების მოთხოვნების დაკმაყოფილებას ახორციელებენ ე.წ. საძიებო მიმითებლები.

საძიებო მიმითებლების მუშაობის პრინციპი *Web*–რესურსების „გასაღები სიტყვით“ ძებნაში მდგომარეობს. მომხმარებელი აღწერს საძებნ რესურსს "გასაღები სიტყვის" საშუალებებით და აძლევს ძებნის დავალებას. საძიებო სისტემა

ანალიზებს თავის ბაზაში შენახულ მონაცემებს და გასცემს მოთხოვნის შესაბამის Web-გვერდების სიას. ჰიპერმიმართებთან ერთად გაიცემა მოკლე ცნობები მოპოვებულ რესურსებზე, რის საფუძველზეც მომხმარებელს შეუძლია შეარჩიოს მისთვის საჭირო რესურსები.

დღეს მსოფლიოში არსებობს დაახლოებით 10 ათასი საძიებო მიმთითებლები. სიის თავში ადგილს იკავებს ორი ათეული საზღვარგარეთული სისტემები: *Alta Vista* (WWW.altavista.com); *Excite* (WWW.excite.com) და სხვა.

რუსეთშიც არსებობს რამოდენიმე ძეგნის მაჩვენებლები, რომელთა შორის უდიდესი და პოპულარულია www.aport.ru, www.yandex.ru და www.rambler.ru, ამჟამად საქართველოში პოპულარულია საძიებო სისტემა google.com.

სხვადასხვა საძიებო მიმთითებლებმა მომხმარებელთა მოთხოვნების დამუშავებისათვის შეიძლება გამოიყენონ სხვადასხვა ინფორმაციული ტექნოლოგიები. ეფექტურად რომ შევასრულოთ WWW-ში ინფორმაციის ძიება, უნდა წარმოვიდგინოთ თვითოეული სისტემის ღირსებები და ნაკლი და ზოგადად მაინც ჩავწვდეთ მათი მუშაობის პრინციპს.

საძიებო მიმთითებლების მუშაობის სამი ეტაპი. საძიებო მიმთითებლის მუშაობა შეიძლება სამ ეტაპად დავეყოთ. მათ შორის ორი ეტაპი მოსამზადებელია და შეუმჩნეველია კლიენტისათვის, მხოლოდ მესამე ეტაპზე ხდება მომხმარებელთან ურთიერთობა, მაგრამ თვითოეულ ამ ეტაპზეა დამოკიდებული საძიებო სისტემის ფუნქციონალური თვისებები და მასთან მუშაობის ეფექტურობა.

პირველადი მონაცემთა ბაზის შეგროვება. პირველ ეტაპზე საძიებო სისტემა ახდენს WWW ინფორმაციული სივრცის

სკანირებას. ამ მიზნით იყენებენ სპეციალურ აგენტურ პროგრამებს - „ჭიაყელა“. საძიებო სისტემის აგენტები არ უნდა აგურიოთ ქსელის კომპიუტერული ვირუსების სახესხვაობაში, რომლებსაც აგრეთვე „ჭიაყელები“ ჰქვიათ. საძიებო სისტემის „ჭიაყელები“ სრულიად უვნებელია სერვერებისა და კლიენტებისათვის. თავისი შინაარსით ის ძალიან ეფექტური, მცირე ზომის ბრაუზერია. მათი ამოცანაა მხოლოდ მოძებნონ ავტომატურად ქსელში Web-რესურსები ჰიპერმიმართების თანმიმდევრობით, და დარწმუნდებიან რა, რომ ეს რესურსი სისტემისათვის უცნობია, გააკეთონ ასლი მონაცემთა ბაზაში. ასევე ხდება ადრე მიღებული დოკუმენტების განახლება, რომლებმაც განიცადეს ცვლილებები წინამდებარე ასლის გადაღების შემდეგ.

სამძებრო „ჭიაყელას“ მუშაობის ეფექტურობაზე ბევრად და დამოკიდებული საძიებო მიმთითებლის შინაარსობრივი ნაწილი. თვითოეული სისტემა იყენებს საკუთარ საძიებო პროგრამას და კონკურენტებისაგან საიდუმლოდ ინახავს მისი მუშაობის ალგორითმს.

მონაცემთა ბაზის ინდექსაცია. ქსელის Web-რესურსებისაგან შეკრებილი მონაცემთა ბაზა კარგი, მაგრამ საძიებო სისტემის ფუნქციონირებისათვის არასაკმარისი საფუძველია. მისი საშუალებით შეიძლება უკვე მოვემსახუროთ კლიენტების მოთხოვნებს, მაგრამ შეუძლებელია ამის სწრაფად გაკეთება. მომხმარებლის მიერ მითითებული გასაღები სიტყვის ძებნა ფართო მონაცემთა ბაზაში მეტად ხანგრძლივი ოპერაციაა. არასასურველია კლიენტის დაყოვნება წამის ნაწილზე მეტი ხანით. ამიტომ შეკრებილი მონაცემთა ბაზა გადის წინასწარ დამუშავებას, ე.წ. ინდექსაციას. ინდექსაციის ეტაპზე იქმნებიან სპეციალიზირებული

დოკუმენტები - საძიებო მიმთითებლები. უმარტივეს მიმთითებელს ვიცნობთ სასწავლო სახელმძღვანელოსთან მუშაობიდან. არა იშვიათად წიგნის ბოლოში მოყვანილია საგნობრივი მიმთითებელი, რომლის საშუალებითაც, ტერმინის მიხედვით, სწრაფად შეიძლება მოიძებნოს გვერდი, რომლებზეც ეს ტერმინია განმარტებული. ანალოგიურადაა მოწყობილი საძიებო მიმთითებლები. საძიებო მიმთითებლის უმარტივეს ტიპს „უკუ ფაილს“ უწოდებენ. ეს უბრალოდ სიტყვარია, რომლებშიაც შედიან Web-რესურსის დათვალიერების დროს შეხვედრილი ყველა სიტყვა. თვითოეული სიტყვის გასწვრივ მითითებულია მიმართვათა სია, რომლებიც უჩვენებენ მონაცემთა ბაზაში შესაბამისი რესურსის ადგილს.

მომხმარებლისაგან გასაღები სიტყვების მიღებისას საძიებო მიმთითებლების გადათვალიერება ძალიან სწრაფად ხდება, რადგან ის წინასწარაა ანბანის მიხედვით მოწყესრიგებული. შედეგად კლიენტი საკმარისად სწრაფად იღებს მითითებათა სიას მისთვის საინტერესო Web-სერვერებით.

საშედეგო სიის რაფინირება. ეს მესამე ეტაპია, რომლის დროსაც ხორციელდება მომხმარებელთან ურთიერთქმედება. ამ ეტაპზე იქმნება მითითებათა სია, რომელიც გადაეცემა მომხმარებელს საშედეგო სიის სახით. მომხმარებლის წარმოდგენა საძიებო სისტემის მუშაობის ხარისხზე პირდაპირაა დამოკიდებული ამ ეტაპზე გამოყენებულ საძიებო ტექნოლოგიებზე.

საშედეგო სიის რაფინირება მდგომარეობს ძებნის შედეგების გაფილტვრასა და რანჟირებაში. გაფილტვრაში იგულისხმება იმ მითითებებისაგან გაცხრილვა, რომლის მიწოდება მომხმარებლისათვის მიზანშეწონილი არაა, უწინარეს ყოვლისა მოწმდება ასლების არსებობა. თუ სისტემა ერთ სიაში ერთი და

იგივე Web რესურსებზე მრავალ მითითებას შეიცავს, ეს მიუთითებს იმაზე, რომ მისმა საშუალებებმა კეთილსინდისიერად იმუშავეს, პირველ ორ ეტაპზე, მაგრამ არაფერი გააკეთეს მესამე ეტაპზე. განმეორებადი მითითებებით გადატვირთული საშედეგო სიები, ართულებენ ნამდვილად სასარგებლო რესურსების შერჩევას.

რაჟინირება მდგომარეობს საშედეგო სიის წარმოდგენის სპეციალური წესრიგის შექმნაში, რომლის დროსაც უფრო მეტად „სასარგებლო“ (საძიებო სისტემის თვალსაზრისით) მითითებები გადაიტანება სიის თავში, ხოლო ნაკლებად სასარგებლო სიის ბოლოში. ამა თუ იმ მითითებების „სარგებლიანობის“ კრიტერიუმის გაგება კლიენტისათვის შეიძლება სრულიად სხვადასხვაგვარი იყოს. სწორედ ამიტომ, ერთ ბაზასთან მომუშავე სხვადასხვა საძიებო სისტემები იძლევიან ძეგნის სხვადასხვა შედეგს. უპირველესად, რაჟინირებისას გაითვალისწინება Web დოკუმენტში გასაღები სიტყვის გამოჩენის რაოდენობა. პრინციპი „რაც მეტია-მით უკეთესია“ საკმაოდ ნათელია მაგრამ არა მთლად კორექტული. ნამდვილად კარგია, როცა საძებნი სიტყვა საკმარისად ხშირად დოკუმენტის პირველ 5-10 აბზაცში გვხვდება, ხოლო დოკუმენტის დანარჩენი ნაწილები ნაკლებად გაითვალისწინება. ძალიან კარგია, როდესაც გასაღები სიტყვა გვხვდება დოკუმენტის სათაურში ან ნახატის ქვეშა წარწერებში.

ინტელექტუალურ სისტემებს შეუძლია აგრეთვე თანმდევი სიტყვების არსებობის შემოწმება. ასე მაგალითად, მრავალი Web-გვერდის შინაარსის ანალიზის შედეგად, რომელიც ჯერ კიდევ ინდექსაციის ეტაპზე შესრულდნენ, შეიძლება დადგინდეს, რომ სიტყვებს „ელექტრონული კომერცია“ ძალიან ხშირად თან

სდევს სიტყვები, „ციფრული ხელმოწერა“ და „საგადასახადო სისტემები“. თუ საძიებო სისტემამ ამის შესახებ იცის, მაშინ მიიღებს რა კლიენტისაგან სიტყვებით-„ელექტრონული კომერცია“ ძებნის დავალებას, იგი სიის თავში განათავსებს იმ *Web*-გვერდებსაც, რომლებშიც აგრეთვე მოიხსენიება ციფრული ხელმოწერა და საგადასახადო სისტემა. ყველგან, სადაც შეიძლება, ავტომატური სისტემები ისწრაფიან დაეყრდნონ „ადამიანურ ფაქტორს“. ავტომატური სისტემისთვის ამის გაკეთება მარტივი არაა, მაგრამ არსებობენ სპეციალური ტექნოლოგიები. ასე მაგალითად, ჯერ კიდევ ინდექსაციის ეტაპზე მაღალი რეიტინგი შეიძლება მიიღონ იმ გვერდებმა, რომლებზედაც მეტი მითითებებია სხვა *Web*-გვერდებიდან. რამდენადაც ჰიპერმიმართვებს ადამიანები ქმნიან, და არა მანქანები, ეს ფაქტი შეიძლება გამოვიყენოთ როგორც სუბიექტური შეფასება იმ დოკუმენტების „სარგებლიანობაზე“, რომლებიც სწირადაა ციტირებული.

ამ წიგნის ფარგლებში არ შეგვიძლია მოვიცვათ ყველა ის მეთოდები, რომლებსაც იყებებენ საძიებო სისტემები მითითებული სიის ფორმირებისათვის, მაგრამ ამ ეტაპის როლი ძნელად შესაფასებელია. მოშინჯეთ რამოდენიმე საძიებო სისტემასთან მუშაობა შეაფასეთ თუ როგორაა აქვთ მათ შედეგების ფილტრაციის და რაჟინირების საქმე. თქვენ, ნამდვილად, შეამჩნევთ, რომ გულმოდგინე ფილტრაცია და გონივრული რაჟინირება აღითქმება მომხმარებლის მიერ, როგორც სისტემის მუშაობის ხარისხის მაჩვენებელი.

2.7 თანამედროვე საძიებო მიმთითებლების ძირითადი პრობლემები.

მსოფლიოს უდიდესი საძიებო მიმთითებლების უმრავლესობა ამჟამად კრიზისულ მდგომარეობაშია. საძიებო სისტემის საერთო კრიზისს აქვს მთელი რიგი ობიექტური მიზეზები. ყველა ისინი დაკავშირებულია ობიექტურ წინააღმდეგობასთან, რომლებიც ინტერნეტის განვითარების პროცესში წარმოიქმნებიან. სხვადასხვა ქვეყნებში ეს კრიზისული მოვლენები სხვადასხვაგვარად გამოვლინდებიან.

საძიებო სისტემებში კრიზისული სიტუაციის განსაზღვრულ ძირითად წინააღმდეგობას წარმოადგენს Web-ინფორმაციული სივრცის და თვით საძიებო სისტემების განვითარების დინამიკის შეუსაბამობა. ადრეულ ეტაპზე, როდესაც საძიებო სისტემები ჯერ კიდევ ყალიბდებოდნენ Web რესურსების მოცვის კოეფიციენტი 50%-ს აღწევდა. 1994 წლისათვის Web-რესურსების რაოდენობა 100 მილიონ Web-გვერდზე მეტს შეადგენდა, რომელთაგანაც ათობით მილიონი ინდექსირებული იყო.

არსებული ინფორმაციული სივრცის მოცვის კოეფიციენტი 2000 წლისთვის 20% არ აღემატებოდა, ამასთან იგი ყოველდღიურად განაგრძობს დაცემას. Web-სივრცე ვითარდება ათობითი მილიონი ადამიანის ძალისხმევით, ხოლო რამოდენიმე საძიებო სისტემა ვერ ასწრებს მათ ინდექსირებას.

მეორე წინააღმდეგობა წმინდად ეკონომიკურია. 1997-2006 წლების მიჯნაზე Web-ინფორმაციული სივრცის განვითარებამ ისეთ მასშტაბებს მიაღწია, რომ მისი ინდექსაციისათვის საჭირო გახდა ბევრად უფრო მძლავრი აპარატურული, პროგრამული და

საკადრო რესურსების მოზიდვა. ამავე პერიოდში მსხვილი ინვესტორების ინტერესები მიმართული იყო ინტერნეტის საინფორმაციო სამსახურებისკენ, რის შედეგადაც მოხდა რიგი საინფორმაციო სისტემების ინვესტირება. ამან კი იმოქმედა მათი მუშაობის ხასიათზე, რადგანაც საძიებო სისტემების ადმინისტრაცია იძულებული იყო ყურადღება მიექცრო არა იმდენად სწრაფად მზარდი *Web*-გვერდის ინდექსაციაზე, არამედ აქციონერების ინტერესების დაკმაყოფილებაზე. მთელმა რიგმა მსხვილმა საძიებო სისტემებმა დაიწყეს ინდექსაციის ხელოვნური დამუხრუჭება და ყურადღება საქმიანობის კომერციულ მხარეზე გაამახვილეს. წარსულში შინაარსობრივად პოპულარული მრავალი საძიებო სისტემები დღეს გარდაიქმნენ მოსახერხებელ და ღამაზ *Web*-პორტალებად (შესასვლელებად), მაგრამ მეცნიერული ძიების ამოცანებს თავს არადამაკმაყოფილებლად ართმევენ.

ინტერნეტის გაფართოებასთან ერთად, იკვეთება კლიენტის ინტერესებთან დაკავშირებული წინააღმდეგობა. მათ უკვე აღარ აწყობთ ჰიპერმიმართვების ამომწურავი სიები, რომლებსაც საჭირო *Web*-რესურებთან მივყავართ. როდესაც საძიებო სისტემები იძლევიან ძალიან ბევრ მიმართვებს, მათი გამოყენება ისევე ძნელია, როგორც ძალიან ცოტასი. კლიენტს უნდა იმდენი „ჰიპერმიმართვა“ რამდენსაც შესძლებს აითვისოს, ამასთან მისთვის სასურველია „ყველაზე საუკეთესო“ მიმართვები. ამანაც მნიშვნელოვნად დაამუხრუჭა *Web*-ის ინდექსაციის სამუშაოები. მრავალმა საძიებო სისტემებმა საერთოდ შეწყვიტეს ინფორმაციის შეგროვება და მისი ანალიზი. ამის ნაცვლად ისინი კლიენტის მოთხოვნებს გადაამისამართებენ ტექნიკურად უფრო კარგად ადჭურვილ საძიებო სისტემებზე, ხოლო თვითონ ყურადღებას

ამახვილებენ მესამე ეტაპზე მიღებული შედეგების ფილტრაციასა და რანჟირებაზე. ასე მაგალითად, მრავალი საძიებო სისტემები ეყრდნობიან საძიებო სისტემას Inktomi (www.Inktomi.com), რომელიც ასრულებს საძიებო ოპერაციებს სხვა საძიებო სისტემების შეკვეთით.

2.8 უახლესი საძიებო ტექნოლოგიები.

ავტომატური კატალოგიზაცია. Web-სივრცის გამოკვლეულ და გამოუკვლევებელ მოცულობებს შორის საძიებო კატალოგებისათვის წინააღმდეგობა უფრო მწვავეა ვიდრე საძიებო მიმთითებლებისათვის. მიუხედავად ამისა, აქ არის პერსპექტიული განვითარების მიმართულება. ისინი დაფუძნებულია ავტომატური კატალოგიზაციის SMART-ტექნოლოგიაზე. არსებობს მრავალი თეორიული გამოკვლევები SMART-ტექნოლოგიების სფეროში, მაგრამ უფრო მეტად პერსპექტიულია ვექტორული ინფორმაციული სივრცის მოდელი. წარმოვიდგინოთ ექსპერტი რაიმე სფეროში მაგალითად, იურისპრუდენციაში თუ მას დავესახავთ ამოცანას, მას შეეძლება შეადგინოს ისეთი სფეროებისათვის დამახასიათებელი ლექსიკონი, როგორცაა საავტორო უფლება, სამოქალაქო სამართალი, სისხლის სამართალი და ა.შ. მრავალი დოკუმენტების გაანალიზებით ამ სფეროდან ის შეძლებს არა მარტო მიუთითოს ამ სფეროსათვის დამახასიათებელი ტერმინები და ცნებები, არამედ მისცეს მათ მნიშვნელობითი შეფასებები. ასე მაგალითად, ნათელია, რომ სიტყვას „ხელშეკრულება“ აქვს უფრო დიდი მნიშვნელობა სამოქალაქო სამართლის დოკუმენტში, ვიდრე სისხლის სამართლის. ტერმინებისა და მნიშვნელობითი კოეფიციენტების კომბინაციით, შეიძლება აიგოს მრავალგანზომი-

ლებიანი კოორდინატთა სისტემა, რომლებშიც შეიძლება აღიწეროს ცოდნის სხვადასხვა სფეროები სხვადასხვაგვარი, მრავალგანზომილებიანი ვექტორებით.

მიიღებს რა ახალ *Web*-გვერდს, საძიებო სისტემას შეუძლია მისთვის ავტომატურად ააგოს შინაარსის ფორმალურ ანალიზზე დაფუძნებული მათემატიკური ვექტორი. შეადარებს რა ამ ვექტორს ცოდნის სხვადასხვა სფეროში უკვე გაანგარიშებულ ვექტორებთან, სისტემას ადამიანის მონაწილეობის გარეშე შეუძლია ივარაუდოს რომელ კატეგორიას, თემას და განყოფილებას მიეკუთვნება ესა თი ის დოკუმენტი.

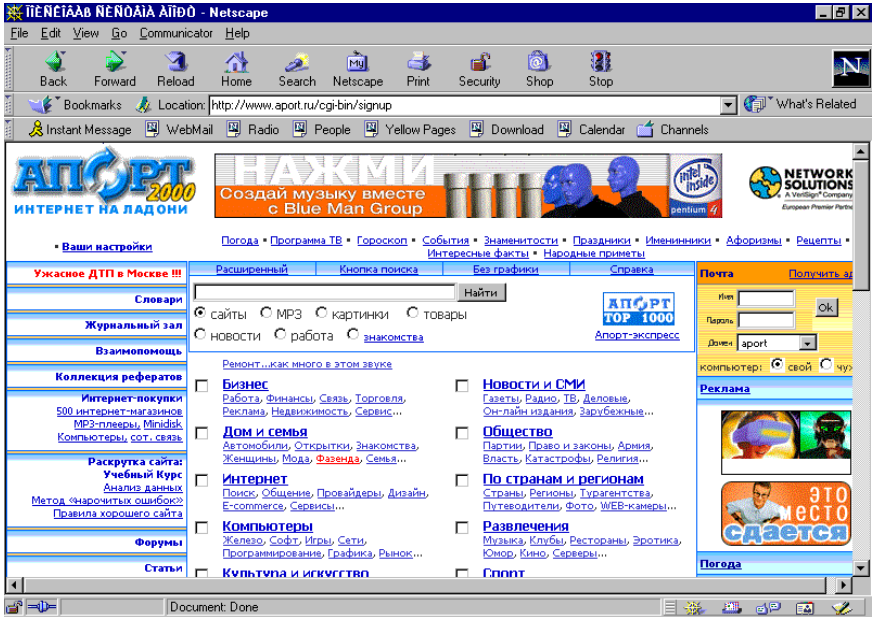
ასეთი მიდგომისას აუცილებელი არაა ყველა ცნობილი *Web*-გვერდის ასლის შენახვა, ასევე საჭირო არაა მათი საძიებო მიმთითებლების შენახვაც. სრულიად საკმარისია თვითთვეული *Web*-დოკუმენტისათვის შეინახოს მხოლოდ მისი *URL* მისამართი და ვექტორის შესაბამისი რიცხვი. ამჟამად *SMART* ტექნოლოგიის კონკრეტული ალგორითმები არ ქვეყნდებიან, ვინაიდან სიახლეს წარმოადგენენ, მაგრამ შეგვიძლია ვივარაუდოთ, რომ ისინი უკვე მუშაობენ მაგალითად რეალური დროის საძიებო სისტემებში, ისეთებში როგორიცაა, *Alexa* (www.alexa.com).

რეალური დროის სისტემები. ინფორმაციის ძებნის ტექნოლოგიაში ამ ახალ მიმართულებას განვიხილავთ საძიებო სამსახურის *Alexa* (www.alexa.com) მაგალითზე. ამ სამსახურთან სამუშაოდ მომხმარებელი უნდა დაუკავშირდეს მის ცენტრალურ სერვერს, მიიღოს მისგან და დააყენოს თავის კომპიუტერზე კლიენტის პროგრამა. ეს პროგრამა მიუერთდება ბრაუზერს და მუშაობს, როგორც დამატებითი პანელი *Microsoft Internet Explorer*-ის ან *Netscape Navigator*-ის ფანჯარაში.

ბრაუზერის ყოველი გაშვებისას კლიენტის პროგრამა კავშირს ამყარებს თავის ცენტრალურ სერვერთან და შემდეგში მუშაობს მასთან წყვილში. იგი სერვერს გადაუზღავნის ყველა იმ *Web*-გვერდების ასლებს, რომელსაც მომხმარებელი მიმართავს, ე.ი. ასრულებს იგივე ფუნქციას, რასაც ავტომატური „ჭიაყელა“, რომელსაც გადაჰქონდა *Web*-რესურსის ასლი ტრადიციული საძიებო სისტემის სერვერზე. მაგრამ ამასთან არის ორი არსებითი განსხვავება:

- ✓ ჯერ ერთი, ადამიანი ინტერნეტში ნავიგაციის დროს არ ხელმძღვანელობს იგივე პრინციპით, რითაც ავტომატური პროგრამა, ამიტომ სერვერი იღებს არა ყველა *Web*-რესურსების ასლებს, არამედ მხოლოდ იმას რამაც დააინტერესა რომელიმე მისი კლიენტებიდან.
- ✓ მეორეს ვხრივ გასაგებია, რომ როდესაც *Web*-რესურსების მიწოდებას ახდენენ რამოდენიმე მილიონი მუდმივი კლიენტი, მაშინ *Web*-სივრცის ინდექსაცია რამდენადმე უფრო სწრაფად ხდება.

თავის მხრივ, აგრეთვე მომხმარებელსაც აქვს მნიშვნელოვანი უპირატესობა. რომელ *Web*-გვერდზეც არ უნდა იყოს იგი, სისტემა ყოველთვის მზადაა შესთავაზოს მას სხვა *Web*-გვერდების სია, რომლებსაც აქვთ მსგავსი შინაარსის თემატიკა. იგი ამზადებს ამ სიას სხვა ადამიანებთან მუშაობით მიღებული გამოცდილების საფუძველზე. ასე შეიძლება მივიღოთ



სურ. 7 რეალური დროის საძიებო სისტემა Aport მოვარი გვერდი გთავაზობთ მიმართულებს Web- გვერდებზე

რეკომენდაციები, რომელთა მოძებნა ძალიან ძნელი იქნებოდა (ზოგჯერ შეუძლებელიც) ტრადიციული საძიებო სისტემებით. რეალური დროის საძიებო სისტემებთან მუშაობა ჩვეულებრივ ნავიგაციას WWW-რესურსებში გადააქცევს მომხიბლავ ინტერაქტიულ კვლევად. სურათზე 7, ნაჩვენებია რეალური დროის საძიებო სისტემის მოვარი გვერდი წიგნის დაწერის მომენტისათვის.

2.9 ეფექტური ძეგნის ხერხები.

რეფერატული ძეგნის ჩასატარებლად, მაშინ როდესაც საძიებო თემა ფართოდაა მოცემული, რეკომენდირებულია ისეთი საძიებო კატალოგების გამოყენება, როგორცაა *Yahoo* (www.yahoo.com) ან *Atrus* (atrus.aport.ru). ისინი საშუალებას გვაძლევენ სწრაფად დავადგინოთ პირველწყაროების ადგილმდებარეობა. პირველწყაროების გაცნობისას საჭიროა, პირველ რიგში, ყურადღება გავამახვილოთ ცნებების ბაზაზე. ძირითადი ცნებების და ტერმინების ცოდნა მოგვცემს საძიებო მიმთითებლებში გასაღები სიტყვების გამოყენებით ჩაღრმავებული ძეგნის საშუალებას.

საძებნ თემაზე პირველადი ცნობების არსებობისას, დოკუმენტები შეიძლება მოიძებნოს საძიებო მიმთითებლებში. ამასთან უნდა განვასხვაოთ *მარტივი*, *გაფართოებული*, *კონტექსტური* და *სპეციალური* ძეგნის ხერხები.

მარტივი ძეგნის ქვეშ იგულისხმება *Web*-რესურსების მოძებნა ერთი ან რამოდენიმე გასაღები სიტყვით. მარტივი ძეგნის ნაკლს წარმოადგენს ის, რომ იგი იძლევა ძალიან ბევრ დოკუმენტს, რომელთა შორის ძნელია ხელსაყრელი დოკუმენტის ამორჩევა.

გაფართოებული ძეგნის გამოყენებისას გასაღები სიტყვებს ერთმანეთს უკავშირებენ ლოგიკური დამოკიდებულობების ოპერატორებით. გაფართოებულ ძეგნას იყენებენ იმ შემთხვევაში, როცა მარტივი ძეგნა ძალიან ბევრ დოკუმენტებს იძლევა. ლოგიკური დამოკიდებულობების საშუალებით ძეგნის დავალებას ისეთნაირად აყალიბებენ, რომ უფრო დეტალურად აღიწეროს დავალება

და შეიზღუდოს შერჩევის სფერო, მაგალითად, გამოქვეყნების თარიღით ან მონაცემების ტიპით.

კონტექსტური ძებნა ზუსტი ფრაზით ძებნაა. ის მოხერხებულია ინფორმაციის რევერატული ძებნისას, მაგრამ ხელმისაწვდომი არაა ყველა საძიებო სისტემებისათვის. ასეთი შესაძლებლობების უზრუნველსაყოფად სისტემა უპირველეს ყოვლისა უნდა მუშაობდეს არა მარტო ინდექსირებულ ფაილებთან, არამედ Web გვერდების სრულფასოვან გამოსახულებასთან. ეს საკმარისად ნელი ოპერაციაა და მას ყველა საძიებო სისტემა ვერ ახორციელებს.

სპეციალური ძებნა გამოიყენება იმ Web-გვერდების მოსაძებნად, რომლებიც შეიცავენ მიმართვებს მიცემულ URL-მისამართებზე, აგრეთვე სამსახურებრივ ველებში, მაგალითად, სათაურის ველში მიწოდებულ მონაცემებს.

2.10 საძიებო სისტემების გამოყენების რეკომენდაციები.

მეცნიერული ძებნის ჩასატარებლად, კერძოდ სამართლის და ეკონომიკის თემაზე, რეკომენდირებულია საძიებო სისტემის *Norther Light* (www.northerlight.com) გამოყენება. ამ სისტემას აქვს Web-სივრცის მოცვისერთოერთი საუკეთესო კოეფიციენტი და მისი ადმინისტრაცია მიმართავს სპეციალურ ძალისხმევას თავისი მიმთითებლების აქტუალობის მხარდასაჭერად. ამას გარდა სისტემა წარმატებით უთავსებს ერთმანეთს საძიებო მიმთითებლისა და კატალოგის თვისებებს. უფრო პოპულარულ თემებზე შეიძლება მოვნახოთ მასში კატალოგის ტიპის სპეციალური განყოფილებები, მათ *Special Editions* უწოდებენ და ხელით მზადდებიან. დამატებით სისტემა გვთავაზობს აქტუალური

მეცნიერული დოკუმენტების მოწოდების ფასიან მომსახურებას. ისინი განთავსებულია განყოფილებაში *Special Collection*.

ყველაზე დიდი საძიებო მიმთითებელი აქვს საძიებო სისტემას *Fast Search (www.alltheWeb.com)*. ამ დროისათვის ის მოიცავს 400 მილიონ უნიკალურ *Web*-გვერდს და ძალიან სწრაფად ვითარდება. საძიებო სისტემა, გაშვების შემდეგ სულ ერთ წელში, ინდექსირებული სივრცის მოცულობის მიხედვით მსოფლიოში პირველ ადგილზე გავიდა და როგორც ვარაუდობენ, 2005 წლისათვის პირველი მილწევს ფსიქოლოგიურ ზღვარს-ერთ მილიარდ უნიკალურ *Web*-გვერდს.

ისტორიულად, მეტად პოპულარულია საძიებო სისტემა *Alta Vista (www.altavista.com)*, მაგრამ 1997 წლიდან მოყოლებული იგი განვითარების დინამიკაში ჩამორჩება და ორიენტაციას იღებს კომერციულ ამოცანებზე. მიუხედავად ამისა, ის კვლავინდებურად ითვლება ერთერთ საუკეთესო საშუალებად კონტექსტური ძებნის ოპერაციებისათვის, თუმცა, სისტემამაც *Fast Search* ბოლო დროს აგრეთვე დაიწყო კონტექსტური ძებნით მომსახურება.

ამჟამად რუსეთში მოქმედებს სამი, სიმძლავრით თითქმის ერთნაირი, საძიებო მიმთითებელი: „*Aport 2000*“ (www.aport.ru), „*rambler*“ (www.rambler.ru) და "yandex" (www.yandex.ru). ისინი ფლობენ თითქმის ერთნაირ „ცოდნას“ ინტერნეტის რუსული სექტორის რესურსებზე და მუშაობენ საკმარისად სწრაფად. სისტემის „*Aport 2000*“ გამოყენება მოხერხებულია მარტივი ძებნის ოპერაციებში, მას გამოარჩევს განსაკუთრებით ყურადღებიანი მიდგომა ფილტრაციისა და რანჟირების შედეგებისადმი. ამ სისტემაში მიღებულია ძებნის სპეციალური ზომები შედეგების

თვალსაჩინო წარმოდგენისათვის, დუბლიკატების გამოსარიცხავად და არააქტუალური მიმართვების მოსაცილებლად.

სისტემა „*Rambler*“ თავისი არსით წარმოადგენს არა მხოლოდ საძიებოს, არამედ ასრულებს მოხერხებული *Web*-პორტალის (მთავარი შესასვლელის) ფუნქციებსაც.

სისტემა „*Yandex*“ გამოყენება მოხერხებულია რთული საძიებო დავალებების ფორმირებისათვის, რამდენადაც იგი ფლობს უფრო მეტად მოქნილ ენას გაფართოებული ძებნისათვის.

თავი 3. ელექტრონული ფოსტა.

ზოგადი მიმოხილვა

ელექტრონული ფოსტა ერთერთი ადრეული ქსელური სამსახურია. მისი თავდაპირველი დანიშნულება მოკლე ტექსტური შეტყობინებების გამგზავნისაგან ადრესატამდე შუალედური საფოსტო სერვერებით გადაცემაში მდგომარეობდა. დღეისათვის ელექტრონული ფოსტის საშუალებით გადაცემა არა მხოლოდ ტექსტური შეტყობინებები, არამედ ნებისმიერი მონაცემთა ფაილები გრაფიკის, ხმის ჩანაწერების ელემენტებითა და სხვა მულტიმედიაური კომპონენტებით. არსებობს აგრეთვე საშუალებები, რომლებითაც იქმნება, რედაქტირდება, გადაიცემა, მიიღება და აღდგება ხმოვანი და ვიდეო შეტყობინებები. დღეისათვის ელექტრონული ფოსტის ფუნქციონალური გაუმჯობესების ერთერთი მიმართულებაა მობილური და ფაქსიმილური კავშირების საშუალებებთან ინტეგრაცია. ამჟამად ელექტრონულ ფოსტასთან მუშაობის ტექნიკური საშუალებები არ შემოიფარგლება მხოლოდ კომპიუტერებით, ტექსტური და ხმოვანი შეტყობინებების გაგზავნისა და მიღებისათვის შეიძლება კავშირის ისეთი საშუალებების გამოყენება, როგორცაა ფიჭური ტელეფონები, პეიჯერები, მობილური გამოთვლითი მოწყობილობები (*Personal Digital Assistant*).

შემავალი და გამომავალი ფოსტის პროტოკოლები.

როგორც ყველა ქსელური სამსახურის, ელექტრონული ფოსტის რეალიზაციაც ხდება პროგრამათა წყვილისა და მათ შორის ურთიერთქმედების პროტოკოლების დახმარებით. ინტერნეტის

მხრიდან მუშაობს პროგრამა-სერვერი, ხოლო მომხმარებლის მხრიდან პროგრამა-კლიენტი. ელექტრონული ფოსტის დამახასიათებელი თავისებურება, რითაც იგი განსხვავდება ინტერნეტის სხვა სამსახურებისაგან, მდგომარეობს იმაში, რომ მისი მუშაობა დაფუძნებულია ორი პროტოკოლის გამოყენებაზე. ერთი გამოიყენება გამომავალი შეტყობინებების გასაგზავნათ, მეორე კი შემავალი კორესპონდენციების მისაღებად. შესაბამისად, ინტერნეტის მხრიდან ელექტრონული ფოსტის მუშაობა უზრუნველყოფილია ორი სერვერით: გამომავალი შეტყობინებების სერვერით და შემავალი შეტყობინებების სერვერით. შემავალი შეტყობინებების სერვერს ხშირად უბრალოდ „საფოსტო ყუთს“ უწოდებენ. ორი განმასხვავებელი პროტოკოლის არსებობის აუცილებლობა დაკავშირებულია უსაფრთხოების მოთხოვნებთან. მაგალითად, შეტყობინებების გადაცემისას ჩვეულებრივ საჭირო არ არის გამგზავნის იდენტიფიკაციის მკაცრი პროცედურა. ანალოგიურ მოვლენასთან გვაქვს საქმე ჩვეულებრივ ფოსტაში, როცა წერილის გაგზავნისათვის საკმარისია კონვერტის ჩაგდება ნებისმიერ საფოსტო ყუთში. გამომავალი შეტყობინებების სამსახური დაფუძნებულია პროტოკოლზე *SMTP (Simple Mail Transfer Protocol-ფოსტის გადაცემის უბარტივესი პროტოკოლი)* და ინტერნეტის მხრიდან უზრუნველყოფილია *SMTP* სერვერებით.

შემავალი შეტყობინებებისას საქმე სხვაგვარადაა. შეტყობინებების მიღებისათვის კლიენტმა უნდა წარმოადგინოს გარკვეული უფლებები. ჩვეულებრივ ფოსტაში შეკვეთილი კორესპონდენციების მიღებისას კლიენტი ან წარმოადგენს დოკუმენტს საფოსტო განყოფილებაში ან მას უნდა ჰქონდეს საკუთარი საფოსტო ყუთის გასაღები (გასაღები არის პიროვნების

იდენტიფიკაციის მექანიკური საშუალება). ელექტრონული ფოსტის შემავალი შეტყობინებების სამსახური ფაქტიურად ასრულებს საფოსტო განყოფილებების როლს. იგი ამოწმებს კლიენტის უფლებებს მისი სარეგისტრაციო სახელისა და პაროლის მეშვეობით, რის შემდეგაც მიაწოდებს მას „საფოსტო ყუთში“ დაგროვილ კორესპონდენციას. ამ სამსახურის შედარებით გაგრძელებულ პროტოკოლს წარმოადგენს *POP3 (Post Office Protocol 3 - საფოსტო განყოფილების ოქმი, ვერსია 3)*.

ელექტრონულ ფოსტასთან მუშაობის ზოგადი წესები

ელექტრონულ ფოსტასთან მუშაობისათვის მომხმარებელმა უნდა შეასრულოს შემდეგი მოქმედებები:

1. დარეგისტრირდეს ელექტრონული ფოსტის ერთ-ერთ სერვერზე, რომელიც ემსახურება როგორც *SPTP*, ისე *POP3* პროტოკოლს. რეგისტრაცია ეწოდება *სააღრიცხვო ჩანაწერის მიღებას*. რეგისტრაციის შედეგად კლიენტი ღებულობს სააღრიცხვო ჩანაწერს *SMTP* და *სააღრიცხვო ჩანაწერს POP3*. თეორიულად ეს ჩანაწერები შეიძლება მიღებული იქნას სხვადასხვა სერვერებზე, მაგრამ ეს მოუხერხებელია და ჩვეულებრივ მათ ღებულობენ *სერვის-პროვაიდერთან*.
2. დააყენოს საკუთარ კომპიუტერზე პროგრამა-ელექტრონული ფოსტის კლიენტი. როგორც წესი, შემავალი და გამომავალი ელექტრონულ ფოსტასთან მუშაობა ხდება ერთი და იგივე პროგრამით, თუმცა ეს აუცილებელი არაა.
3. გამართოს საფოსტო კლიენტი სააღრიცხვო ჩანაწერებთან *SMTP* და *POP3* სამუშაოდ. გამართვის დროს პროგრამაში

შეიტანება მომხმარებლის სარეგისტრაციო მონაცემები (სარეგისტრაციო სახელი და პაროლი), რომლებიც მიიღება ელექტრონული ფოსტის მომსახურების მიმწოდებელთან ხელშეკრულების დადებისას. ეს მოსახეხრხებელია, რათა POP3 სერვერთან მიერთებისას პროგრამას შეეძლოს სერვერს ავტომატურად წარუდგინოს უფლებები და ყოველთვის არ იყოს აუცილებელი მონაცემების ხელით შეტანა.

კლიენტის პროგრამული უზრუნველყოფის გამართვის შემდეგ მომხმარებელს შეუძლია მისი საშუალებით შექმნას შეტყობინებები, შეიტანოს მიმღების ელექტრონული ფოსტის მისამართი და გასცეს გაგზავნის ბრძანება.

შემდეგში შეტყობინება მოძრაობს საფოსტო სერვერების გავლით გამგზავნის SMTP-სერვერიდან მიმღების POP3-სერვერამდე, სადაც გროვდება მიღებული შეტყობინებები იმ მომენტამდე, ვიდრე ადრესატი მოახდენს სერვერთან დაკავშირებას.

თავის „საფოსტო ყუთთან“ დაკავშირების მომენტში ადრესატს შეუძლია მიიღოს:

- ✓ შეტყობინება საფოსტო გზავნილების არსებობის შესახებ;
- ✓ სამსახურებრივი ინფორმაცია, რომელიც მიიღება შეტყობინების სათაურის ველიდან (გამგზავნის სახელი, გაგზავნის თარიღი, შეტყობინების ზომა და თემა და ა.შ.);
- ✓ შეტყობინების სრული ტექსტი.

კერძოდ რას მიიღებს ადრესატი, დამოკიდებულია იმაზე, თუ როგორაა მომართული მისი კლიენტის პროგრამა. მას არ შეუძლია მართოს სერვერზე „საფოსტო ყუთში“ მიღებული ინფორმაციის მოცულობა და შემაღვენლობა, მაგრამ მას

შეუძლია მართოს რა მოცულობით მოხდეს ამ ინფორმაციის ტრანსპორტირება მის კომპიუტერში. ეს შესაძლებელია, თუ მისი პროგრამა-კლიენტი აღჭურვილია სათანადო ფუნქციებით.

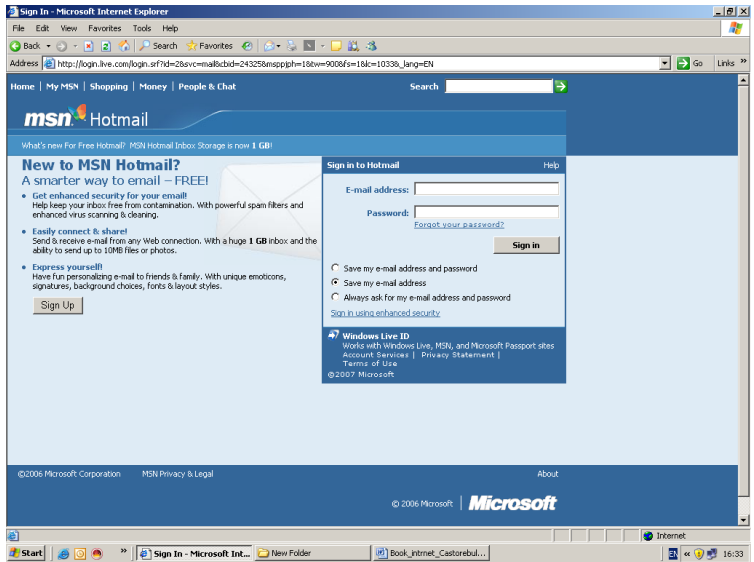
WWW-ზე დაფუძნებული ელექტრონული ფოსტა

SMTP და *POP3* ოქმებზე დაფუძნებულ „ჩვეულებრივ“ ელექტრონულ ფოსტას E-Mail ეწოდება. მასთან ერთად ბოლო წლებში შეიქმნა და განვითარდა WWW სამსახურზე დაფუძნებული ინტერნეტის ელექტრონული ფოსტის სისტემაც, რომელსაც Web-Mail ეწოდება. ეს არის არა დამოუკიდებელი სამსახური, არამედ *World Wide Web* სამსახურის საშუალებებით რეალიზებული სერვისი, ჩვენს მიერ განხილული ოქმის *HTTP*-ს საფუძველზე. ინტერნეტის მხრიდან ეს სერვისი წარმართება ჩვეულებრივი Web-სერვერით, ხოლო კლიენტის მხრიდან მასთან სამუშაოდ საკმარისია ჩვეულებრივი Web-ბრაუზერის ქონა. ეს მოსახერხებელია მათთვის, ვინც კარგად აითვისა Web-ბრაუზერთან მუშაობა და არ სურს დროის დაკარგვა ელექტრონული ფოსტის სპეციფიკური პროგრამული საშუალებების ასათვისებლად.

Web-Mail არის ძველი, დამოუკიდებელი სამსახურის E-Mail-ის მუშაობის Web-ტექნოლოგიით წარმართვა მისი ფუნქციების სრული ნაკრების შენარჩუნებით, ისე, რომ მომხმარებლისათვის განსხვავება გამოვლინდება მხოლოდ იმაში, რომელი პროგრამები გამოიყენება მუშაობისათვის, და იმაშიც თუ როგორ სრულდება სამსახურთან ჩართვა.

Web-Mail ელექტრონულ ფოსტასთან მუშაობის ზოგადი წესები დგომარეობს შემდეგ ში:

1. Web-Mail ელექტრონული ფოსტის საადრიცხვო ჩანაწერი იქმნება სამსახურის Web-კვანძში. მასთან ჩართვა ხდება ბრაუზერის დახმარებით ჩვეულებრივად URL-მისამართზე გადასვლით. რეგისტრაცია სრულდება ერთ-ერთ Web-გვერდზე HTML - ფორმის შევსების გზით.
2. საფოსტო შეტყობინების მომზადება და გაგზავნა სრულდება Web-ფორმის ველების შევსების გზით. შემდეგში შეტყობინება გადაეცემა მითითებული მისამართით. შექმნილი შეტყობინებები ფაქტიურად



3.

სურ 1. „საფოსტო ყუთის“ რეგისტრაცია Hotmail.com სამსახურში

წარმოადგენს HTML დოკუმენტებს და მათი დათვალიერება ხდება ნებისმიერი ბრაუზერით. როგორც HTML დოკუმენტებს, მათ შეიძლება ჰქონდეთ შრიფტული და ფერადი

ფორმატირება, ფონური გამოსახულება, გრაფიკა და სხვა ობიექტები. შორეული აღმოსავლეთისა და სამხრეთ-აღმოსავლეთ აზიის ქვეყნებისათვის Web-ზე დაფუძნებული ელექტრონული ფოსტის უპირატესობაა ის, რომ შეტყობინებებში შეიძლება გამოყენებული იქნას სიმბოლოთა ნაკრები, რომელშიც თითოეული სიმბოლოს კოდირება ხდება ორი ბაიტით. ეს ნიშნავს, რომ HTML ფორმატში შეიძლება გადაიგზავნოს შეტყობინება ჩინურ, იაპონურ, კორეულ და სხვა იეროგლიფური სიმბოლოების ენაზე. თუ დაიშვება, რომ ადრესატს არა აქვს სააღრიცხვო ჩანაწერი Web-სერვერზე და იყენებს „ჩვეულებრივ“ ელექტრონულ ფოსტას სააღრიცხვო ჩანაწერით POP3 სერვერზე, მაშინ შეტყობინების ფორმატი ავტომატურად გარდაიქმნება ჩვეულებრივ ტექსტად. თუმცა დღეისათვის POP3 სააღრიცხვო ჩანაწერით მომუშავე ბევრ საფოსტო კლიენტსაც აქვს შესაძლებლობა აღადგინოს შეტყობინება HTML ფორმატში.

4. Web-Mail-ის მისამართზე მიღებული შეტყობინებები ინახება სერვერზე და მათი დათვალიერება შეიძლება ბრაუზერის საშუალებით, როგორც ჩვეულებრივი Web-გვერდებისა. აუცილებლობის შემთხვევაში შეიძლება მათი კოპირება ხისტ დისკზე, ამის გაკეთება აუცილებელი არ არის. საკუთარი „საფოსტო ყუთი“ Web-სერვერზე შეიძლება განიხილებოდეს როგორც დაშორებული Web-პააკები და საერთოდ არ მოხდეს ინფორმაციის შენახვა კომპიუტერში.

ელექტრონული ფოსტის შეტყობინებების სტრუქტურა.

ელექტრონულ ფოსტასთან მუშაობისას მიღებული არ არის ყოველი ცაკლეული შეტყობინების („წერილის“) , როგორც დამოუკიდებელი დოკუმენტის განხილვა და მისთვის ცაკლე ფაილის გამოყოფა, თუმცა საფოსტო კლიენტებში არსებობს ფუნქცია, რომელიც ამის საშუალებას იძლევა. მიღებულია ელექტრონული ფოსტის შეტყობინებების მონაცემთა ბაზის ცაკლეული ჩანაწერებად განხილვა. ამ აზრით „საფოსტო ყუთი“ POP3 წარმოადგენს დაშორებულ მონაცემთა ბაზას, ხოლო კომპიუტერზე მიღებული შეტყობინებები ქმნიან ლოკალურ მონაცემთა ბაზას. შეტყობინებების მიღება და გაგზავნა ექვივალენტურია ერთი ბაზიდან მეორეში ჩანაწერების კოპირების ოპერაციისა, ხოლო ელექტრონულ ფოსტასთან მუშაობის პროგრამაკლიენტი თავისი ბუნებით წარმოადგენს მონაცემთა განაწილებულ ბაზასთან მუშაობის საშუალებას.

მაშასადამე, თითოეული შეტყობინება - მონაცემთა ბაზის ცალკეული ჩანაწერია. როგორც ყველა ჩანაწერს, მასაც აქვს ველები. ცალკეული ველების ჩანაწერების შემადგენლობაზე შეიძლება ვიმუშაოდ ცალცალკე სხვა შემადგენლობისაგან დამოუკიდებლად. ელექტრონული ფოსტის ეს თავისებურება აქტიურად გამოიყენება ფოსტის კლიენტების მიერ, რასაც შემდგომში დავინახავთ.

შეტყობინების სათაური. ყველაზე მარტივი გაგებით ელექტრონული ფოსტის შეტყობინება ორი განყოფილებისაგან შედგება: შეტყობინების სათაური და შეტყობინების „ტანი“. სათაურს აქვს ველები: To (ვის-ადრესატის სახელი); CC (ასლი-აქ მოიცემა იმ ადრესატების სახელები, ვისთვისაც განკუთვნილია

მოცემული წერილის ასლი), *Subject* (თემა-აქ მოკლედ მოიცემა შეტყობინების თემა) და სხვა. სათაურის ველებს შორის არის თარიღის ველი, აგრეთვე ველი, რომელშიც შეიტანება ინფორმაცია შეტყობინებაში *ჩალაგებული ფაილების* არსებობის შესახებ. საფოსტო ჩალაგებების მექანიზმი საშუალებას იძლევა ტექსტურ შეტყობინებებთან ერთად გადაიგზავნოს არატექსტური ბუნების დოკუმენტები, მაგალითად, მულტიმედიის, არქივის, პროგრამული და სხვა ფაილები.

შეტყობინების ძირითადი განყოფილება. ძირითად განყოფილებაში, რომელსაც აგრეთვე შეტყობინების „ტანს“ უწოდებენ, მოცემულია ძირითადი შინაარსობრივი ტექსტი. პირობითად მასში შეიძლება გამოიყოს ისეთი კომპონენტები, როგორცაა *მიმართვა* და *ხელმოწერა*. თუმცა ისინი წარმოდგენილი არ არის ცაკლეული ველებით და განლაგებულია იქვე, სადაც შეტყობინების ტექსტია, მათ ხანდახან განიხილავენ ცალკე, რამდენადაც ელექტრონული ფოსტის ბევრი კლიენტი იძლევა მათი შექმნის ავტომატიზების შესაძლებლობას.

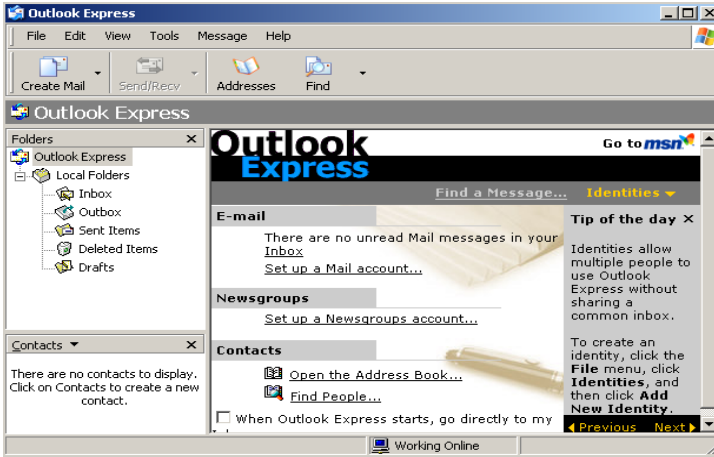
საფოსტო კლიენტების ფუნქციები და თვისებები.

ამჟამად მსოფლიოში გავრცელებულია ელექტრონული ფოსტის კლიენტების რამოდენიმე ასეული პროგრამა. ისინი ერთმანეთისაგან განსხვავდებიან აპარატულ-პროგრამული პლატფორმით, მომხმარებლის ინტერფეისის და შესასრულებელი ფუნქციების შემადგენლობით. Windows-ის პლატფორმისათვის შედარებით პოპულარულ საფოსტო კლიენტებს წარმოადგენენ სისტემები:

- ✓ Microsoft Outlook, რომელიც შედის Microsoft Office პაკეტის შემადგენლობაში;
 - ✓ Microsoft Outlook Express, რომელიც შედის ოპერაციული სისტემა Microsoft Windows-ის შემადგენლობაში სტანდარტული დანართის უფლებით);
 - ✓ Eudora (www.eudora.com);
 - ✓ Pegasus Mail (www.pegasus .usa.com)
 - ✓ The Bat! (www.ritulabs.com)
- საფოსტო კლიენტების განხილვისას შეიძლება გამოიყოს:
- ✓ საბაზო, ძირითადი ფუნქციები;
 - ✓ დამატებითი, გაფართოებული ფუნქციები;
 - ✓ სპეციალური ფუნქციები.

საფოსტო კლიენტების საბაზო ფუნქციები. საფოსტო კლიენტების საბაზო ფუნქციების დანიშნულებაა ელექტრონული ფოსტის შეტყობინებების გაგზავნისა და მიღების უმარტივესი ფუნქციების შესრულება.

შეტყობინებების მიღება და ავტომატური დათვალიერება ყველა საფოსტო კლიენტის ძირითადი ფუნქციაა. POP3 სერვერზე ჩართვის შემთხვევაში წარმოებს ყველა მიღებული შეტყობინებების ავტომატური კოპირება საფოსტო კლიენტის მონაცემთა ბაზაში, რის შედეგადაც შეიძლება მათი წაკითხვა ავტომატურ რეჟიმში (ან ქსელიდან გამორთვისას).



სურ 2. საფოსტო კლიენტის ფანჯრის სტრუქტურა Outlook Express

ახალი შეტყობინებების შექმნა საფოსტო კლიენტის მეორე მნიშვნელოვან ფუნქციაა. მისი რეალიზაციისათვის პროგრამას შეუძლია ჰქონდეს ჩაშენებული ტექსტური რედაქტორი. რედაქტორის ფუნქციონალობა დამოკიდებულია კონკრეტული პროგრამის თვისებებზე. Windows ოპერაციულ სისტემაში მომუშავე საფოსტო კლიენტებისათვის მიღებულად ითვლება ოპერაციების წარმართვა ბუფერის გამოყენებით (ფრაგმენტების გადატანა სხვა დოკუმენტებიდან კოპირებითა და ჩასმით) და ტექსტის კოდირების არჩევის შესაძლებლობით.

შეტყობინებების მოწესრიგება. შემაჯავლი და გამომაჯავლი შეტყობინებების მოწესრიგება წარმოებს დაჯგუფებისა და დახარისხების გზით. დაჯგუფება სრულდება შეტყობინებების განაწილებით ლოგიკურ საქაღალდეებში. შეგახსენებთ, რომ ფიზიკურად ყველა შეტყობინებება ინახება საერთო მონაცემთა ბაზის ერთ ფაილში. მათი გადანაწილება საქაღალდეებში ბაზის

ჩანაწერების გაფილტვრის ექვივალენტური ლოგიკური ოპერაციაა. ყოველი საქაღალდე-ფილტრია, როგორც მაგალითად, საქაღალდეში *Inbox* (შემავალი) აისახება მხოლოდ მიღებული შეტყობინებები, საქაღალდეებში – *Sent* (გაგზავნილი) გაგზავნილი *Outbox* - გასაგზავნათ მომზადებული შეტყობინებები, მაგრამ ჯერ-ჯერობით რაიმე მიზეზით გაუგზავნელი. ბევრი საფოსტო კლიენტი ქმნის სპეციალურ საქაღალდეს *Drafts* (შავი პირი) ისეთი შეტყობინებების შესანახად, რომლებიც არ არის მზად გასაგზავნად. დახარისხება ფილტრაციის შემდეგ გამოიყენება საქაღალდეებს შიგნით შეტყობინებების მოწესრიგებისათვის. დახარისხების ჩვეულებრივი თანმიმდევრობაა - თარიღის მიხედვით, თუმცა იგი შეიძლება შეიცვალოს, თუ საფოსტო კლიენტს აქვს შესაბამისი ფუნქციები.

საპასუხო შეტყობინებების მომზადების ავტომატიზაცია

საპასუხო შეტყობინებების მომზადებისას საფოსტო კლიენტს შეუძლია გამოიყენოს საწყისი შეტყობინების სათაურის ველიდან აღებული მონაცემები. ეს ამარტივებს ველების, ვის - *To*, თემა - *Object* და ა.შ. შევსებას. აღარ არის აუცილებელი ასევე მიმღების მისამართის ხელით შეტანა.

მოსახერხებლად ითვლება საწყისი შეტყობინებების ციტირების ფუნქცია. იგი შესაძლებლობას იძლევა პასუხის მომზადებისას გამოყენებული იქნას საწყისი შეტყობინებიდან არჩეული ფრაგმენტები და შეიქმნას საპასუხო ტექსტი.

ოპერაციები ჩალაგებული ფაილებით

თავისი ბუნებით ელექტრონული ფოსტა განკუთვნილია წმინდა ტექსტური შეტყობინებების გადასაგზავნად, რომლებიც უპირატესად ინგლისურ ენაზეა შესრულებული, ანუ სიმბოლოებით, რომლებიც შედის *ASCII* სტანდარტში. ამ სიმბოლოების განმასხვავებელი თავისებუ-

რება მდგომარეობს იმაში, რომ მათი კოდები არ აღემატება 127-ს. ამავე დროს ნებისმიერ ფაილში (პროგრამულ, საარქივო, მულტიმედიაურ, ფორმალიზებული დოკუმენტების ფაილებში და სხვა) შეიძლება იყოს ბაიტი კოდით 128-იდან 255-მდე მნიშვნელობით. მათი გადაგზავნისათვის ელექტრონული ფოსტის შეტყობინებასთან ერთად საჭიროა სპეციალური გარდაქმნა, რის შედეგადაც სიმბოლოები კოდებით 128-დან 255-მდე იცვლება სიმბოლოების კომბინაციით კოდებით 0-დან 127-მდე. ადრესატის მხარეს საფოსტო კლიენტი ასრულებს შებრუნებულ გარდაქმნას.

თავისუფალი ფაილების გადაგზავნის ასეთ მექანიზმს *საფოსტო ჩალაგებებს* უწოდებენ. ელექტრონული ფოსტის შეტყობინების მომზადებისას გამგზავნი მიუთითებს მისაერთებელი ფაილის განლაგების ადგილს. ამასთან საფოსტო კლიენტი ასრულებს შესაბამის ჩანაწერს შეტყობინების სათაურის ერთ-ერთ ველში, სადაც მიუთითებს ფაილის სახელსა და გამოყენებული კოდირების მეთოდს. კოდირების ძირითადი მეთოდებია: *MIME*, *BinHex* და *UUEncode*. თანამედროვე საფოსტო კლიენტების უმრავლესობას შეუძლია გაიგოს ყველა ეს მეთოდი.

შეტყობინების მიღებისას საფოსტო კლიენტი საშუალებას იძლევა გამოცალკევდეს საფოსტო ჩალაგებები და მოხდეს მისი შენახვა ავტონომიური ფაილის სახით მითითებულ ადგილზე.

საფოსტო კლიენტების დამატებითი ფუნქციები

ელექტრონული ფოსტის კლიენტების (პროგრამების) დამატებითი ფუნქციების დანიშნულებაა მომსახურების ოპერაციების ავტომატიზაციის უზრუნველყოფა ან მოცემულ სამსახურთან მუშაობის გაუმჯობესება.

საიდენტიფიკაციო ჩანაწერების უზრუნველყოფა. საიდენტიფიკაციო ჩანაწერი ეწოდება კონკრეტულ მომხმარებელზე ორიენტირებული პროგრამების გამართვების ერთობლიობას. თუ პროგრამასთან მუშაობს რამოდენიმე ადამიანი, მაშინ ზოგიერთი საფოსტო კლიენტი თითოეულს საშუალებას აძლევს შექმნას საკუთარი საიდენტიფიკაციო ჩანაწერი და ამით მიიღოს ლოგიკური საქაღალდეების საკუთარი კომპლექტი. მხედველობაში მიიღება რომ საფოსტო სერვერთან მიერთებისას ხდება მხოლოდ იმ შეტყობინებების ჩატვირთვა, რომლებიც განკუთვნილია მიმდინარე საიდენტიფიკაციო ჩანაწერის მფლობელისათვის. მომხმარებლის შეცვლისას ხდება საიდენტიფიკაციო ჩანაწერის შეცვლა და მაშინ შესაძლებელია სხვა მიღებული შეტყობინებების კოპირება. უსაფრთხოების დაცვის მიზნით საიდენტიფიკაციო ჩანაწერის შეცვლის ოპერაციას შეიძლება თან ახლდეს პაროლის მოთხოვნა.

სააღრიცხვო ჩანაწერების უზრუნველყოფა. სააღრიცხვო ჩანაწერი ეწოდება კონკრეტულ მიმწოდებელზე ელექტრონული ფოსტის მომსახურების გამართვების ერთობლიობას. თუ მომხმარებელს აქვს სხვადასხვა სერვერზე გახსნილი რამოდენიმე „საფოსტო ყუთი“, მაშინ ზოგიერთი საფოსტო კლიენტი საშუალებას იძლევა აირჩიოს მიმდინარე სააღრიცხვო ჩანაწერი და მარტივად მოხდეს მათ შორის გადართვა.

WWW-ს სააღრიცხვო ჩანაწერების უზრუნველყოფა. თუ საფოსტო კლიენტი იყენებს Web-Mail სააღრიცხვო ჩანაწერებთან მუშაობას, მაშინ მისი გამოყენება შესაძლებელია, როგორც „ჩვეულებრივ“ ელექტრონულ ფოსტასთან სამუშაოდ ასევე ინტერნეტზე დაფუძნებული ელექტრონული ფოსტის სამსახურის „სა-

ფოსტო ყუთებზე“ მისამართავად. ეს ფუნქცია დამახასიათებელია Web-ბრაუზერის ფუნქციებით აღჭურვილი ან Web-ბრაუზერან ინტეგრირებული საფოსტო კლიენტებისათვის.

HTML-ფორმატთან მუშაობა, თუ საფოსტო კლიენტი იყენებს დოკუმენტების HTML-ფორმატს, ეს საშუალებას ქმნის მომზადდეს, გაიგზავნოს, მიიღოს და დათვალიერდეს შეტყობინებები, რომელშიც არის გაფორმების ისეთი ელემენტები, როგორიცაა შრიფტული და ფერადი გაფორმება, ჩაღებული მულტიმედია ობიექტები და სხვა.

სამისამართო წიგნთან მუშაობა, საფოსტო პროგრამაში სამისამართო წიგნი არის საფოსტო მისამართების მონაცემთა ბაზის მართვის საშუალება, რომლიც ემსახურება კონტაქტების აღრიცხვას. *კონტაქტები* ეწოდება სამისამართო წიგნის ჩანაწერებს, რომელსაც ქმნის რეგულარული კორექსონდენტი და შეიცავს მონაცემებს ადამიანებსა და მათი ელექტრონული ფოსტის მისამართებზე. სამისამართო წიგნთან მუშაობის სტანდარტული ფუნქციებია:

- ✓ კონტაქტის ავტომატიზირებული შექმნა მიღებული შეტყობინებების სათაურის ველიდან აღებული მონაცემების საფუძველზე.
- ✓ ახალი შეტყობინებების შაბლონის ავტომატიზებული შექმნა საჭირო კონტაქტის არჩევის შემდეგ;
- ✓ კონტაქტების სიის მოწესრიგება დაჯგუფებისა და დახარისხების გზით.

ჩადგმული ტექსტური რედაქტორის გაფართოებული ფუნქციები

ტექსტური რედაქტორის თვისებებიდან ყველაზე სასურველ ფუნქციას წარმოადგენს განსაკუთრებით მრავალენოვანი მართლწერის შემოწმების საშუალებების არსებობა. დამატებით ფუნქციებში შეიძლება შედიოდეს მიკრობრძანებები მიმართვებისა და ხელმოწერების შესატანად, ასევე ხელმოწერების გენერაციის საშუალებები, მათ შორის, შემთხვევითი ამორჩევის გზით წინასწარ მომზადებული გარე ტექსტური ფაილებიდან. ამ ხერხებით სარგებლობენ საფოსტო შეტყობინებების „გასაფორმებლად“ მათში დამამთავრებელი ციტატების, აფორიზმების, ანდაზების ჩართვისათვის.

შეტყობინებების ფუნქციები. ჩვეულებრივ ამ ფუნქციების რეალიზაცია ხდება დამატებითი სისტემით, რომელიც განკუთვნილია POP3 და Web-Mail სერვერებზე სააღრიცხვო ჩანაწერების მდგომარეობის შესამოწმებლად. განასხვავებენ შეტყობინების ქსელურ და ავტონომიურ საშუალებებს. ქსელური საშუალებები მუშაობენ ინტერნეტთან კავშირის სეანსების დროს და ახორციელებენ სააღრიცხვო ჩანაწერების პერიოდულ გამოკითხვას. შეტყობინებების ავტონომიური საშუალებები მუშაობენ დადგენილი განაწესით, ამასთან მათ შეუძლიათ დამოუკიდებლად დაამყარონ დაშორებული შეღწევის კავშირი და სააღრიცხვო ჩანაწერების შემოწმების შემდეგ გაწვიტონ იგი. შეტყობინებების შედარებით განვითარებულ საშუალებებს შეუძლიათ გაანალიზონ მიღებული შეტყობინების სათაური და მოახდინონ შეტყობინების გადამისამართება ელექტრონული ფოსტის სხვა მისამართზე (იქ, სადაც მოცემულ მომენტში იმყოფება სააღრიცხვო ჩანაწერის მფლობელი) ან კავშირის სხვა საშუალებებზე (ჩვეულებრივი ან

ქსელური ტელეფონი, პეიჯერი, ფაქსმანქანა). ამასთან ზოგიერთ პროგრამას შეუძლია მიღებული ტექსტის გახმოვანებაც.

შეტყობინების სიგნალის სახით შეიძლება გამოყენებული იქნეს ხმოვანი ან ვიზუალური სიგნალი (დიალოგური ფანჯარა). ახალი ფოსტის მიღების შესახებ შეტყობინებების საშუალებათა უმრავლესობას შეუძლია სიგნალის მიცემა მოცემული პროგრამის გაშვებისას, ზოგიერთს კი ფრიად ეგზოტიკური საშუალებით, მაგალითად კლავიატურის შექდიოდების ციმციმით.

„საფოსტო ყუთების“ მართვის საშუალებები. სათაურის ველში მოცემული მონაცემების დამახასიათებელი განსხვავება შეტყობინების „ტანის“ მონაცემებისაგან მათი მცირე ზომებია. იმ შემთხვევაში, როცა ყოველდღიურად მიღებული შეტყობინებების მოცულობა მნიშვნელოვანია, მიზანშეწონილია იმ საფოსტო კლიენტის გამოყენება, რომელიც აღჭურვილია სერვერიდან შეტყობინების ჩატვირთვამდე სათაურის ველების წინასწარი დათვალიერების ფუნქციებით. ეს საშუალებას იძლევა არ მოხდეს ისეთი კორესპონდენციების ჩატვირთვა, რომელიც არ იყო მოთხოვნილი, თავიდან იქნას აცილებული საფოსტო ჩაღებებით არასასურველი ფაილების მიღება, წაშლილი იქნას შეუვსებელ ველებიანი შეტყობინებები. შერჩევისა და წაშლის ყველა ოპერაცია სრულდება უშუალოდ სერვერზე, რაც ამცირებს კავშირის არსების დატვირთვას და მათი ექსპლუატაციის ხარჯებს.

შეტყობინებების გაფილტვრა. სათაურის ველების ზემოთ აღწერილი ანალიზი შეიძლება ჩატარდეს ავტომატურად პროგრამული ფილტრების დახმარებით. ასე მაგალითად, საფოსტო კლიენტები, რომელთაც აქვთ ფილტრაციის საშუალებები არასასურველ შეტყობინებებს ავტომატურად შლიან და ადრესატი მათ

არასოდეს ნახავს, ხოლო გამგზავნი არ მიიღებს ცნობას იმის შესახებ, რომ მისი შეტყობინება მიღებულია და წაკითხულია.

გაფილტვრა გამოიყენება "სპამის" ნეგატიურ მოვლენასთან საბრძოლველად. სპამი - ესაა მოუთხოვნელი კორესპონდენციის დაგზავნა. არსებობს სხვადასხვა შეხედულება სპამის კვალიფიკაციისადმი. კერძოდ, პირველი მიმართვა, როგორც წესი, სპამად არ ითვლება - მას არც თუ იშვიათად იყენებენ ელექტრონული ვაჭრობის სარეკლამო სამსახურები, მაგრამ არამოტივირებული განმეორებითი მიმართვა უკვე ითვლება ელექტრონული ფოსტით სარგებლობის წესების დარღვევად და შეიძლება გასაჩივრდეს.

გაფილტვრის კიდევ ერთი სასარგებლო ფუნქციაა მიღებული შეტყობინებების ავტომატური დაჯგუფება თემატურ ან პერსონალურ ფოლდერებში. ასე მაგალითად, ველის To (ვის) შინაარსის გაანალიზებისას პროგრამას შეუძლია გაანაწილოს მიღებული ფოსტა სხვადასხვა მომხმარებლის შესაბამის ფოლდერებში. ამ ფუნქციას იყენებენ მცირე დაწესებულებებში, როცა რამოდენიმე თანამშრომელი იყენებს ელექტრონული ფოსტის ერთ საერთო საადრიცხვო ჩანაწერს.

„შავი“ და „თეთრი“ სიების უზრუნველყოფა. გაფილტვრის საშუალებებს შეუძლიათ იმუშაონ საფოსტო მისამართების წინასწარ მომზადებულ სიებთან. „შავი“ ეწოდება ელექტრონული ფოსტის მისამართების სიას, რომელთაგან მიღებული შეტყობინებებიც ავტომატურად დაიბლოკება და ნადგურდება უშუალოდ სერვერზე ლოკალურ კომპიუტერში ჩატვირთვის გარეშე. „თეთრი“ სია კი გამოიყენება არჩეული შეტყობინებების გასაშვებად იმ

შემთხვევებში, როცა საფოსტო კლიენტი მომართულია ყველა მიღებული შეტყობინების ბლოკირებაზე.

დღეისათვის ინტერნეტში არის სამსახურები, რომლებიც აღრიცხავენ ელექტრონული ფოსტის ეტიკეტის დამრღვევ ცნობილ სპამერებს და სარეკლამო სამსახურებს. საფოსტო კლიენტს შეუძლია ავტომატურად შეადაროს შემომავალი შეტყობინებების გამომგზავნების მისამართები ქსელური სამსახურების მონაცემებს და მათი რეკომენდაციების საფუძველზე დაბლოკოს მიღებული კორესპონდენციები.

სამუშაოს შესრულებაზე თვითვალისა და კონტროლის ფუნქციები ორგანიზაციებისათვის, რომლებიც მოქალაქეებისაგან ან სხვა ორგანიზაციებისაგან ელექტრონული ფოსტის საშუალებით იღებენ შეტყობინებების (მიმართვების) დიდ ნაკადს, მნიშვნელოვანია შემომავალი დოკუმენტების მოძრაობისა და შესრულების ეფექტური კონტროლი. დიდ ორგანიზაციებში, რომლებიც წელიწადში ათასობით მიმართვას ამუშავებენ ამ მიზნით გამოიყენება საქმისწარმოების მართვის სპეციალური სისტემები. მცირე და საშუალო ორგანიზაციებში ხშირ შემთხვევაში ხერხდება იმ საფოსტო კლიენტით დაკმაყოფილება, რომელსაც აქვს შემსრულებლების ადგილების მიხედვით შემომავალი შეტყობინებების მოძრაობის კონტროლის შესაბამისი ფუნქციები.

რეზერვირებისა და არქივაციის ფუნქციები იმ შემთხვევებში, როცა ორგანიზაციის ელექტრონული ფოსტა გამოირჩევა განსაკუთრებით მნიშვნელოვანი დოკუმენტაციით, მაშინ იყენებენ ელექტრონული ფოსტასთან მუშაობის იმ საშუალებებს, რომელთაც აქვთ მონაცემების შემჭიდროებულ ფორმატში ავტომატური რეზერვირებისა და არქივაციის ფუნქციები. ასეთი ფუნქციების

არსებობა მნიშვნელოვნად ამაღლებს საფოსტო პროგრამის საიმედოობასა და მდგრადობას. ასე მაგალითად, საფოსტო პროგრამის მწყობრიდან გამოსვლის შემთხვევაში საშუალება იქმნება მთლიანად აღდგენილი იქნას მთელი მიმოწერა სამისამართი წიგნის მონაცემების ჩათვლით.

პასუხების ავტომატური გენერაციისა და გადამისამართების ფუნქციები. მიღებულ საფოსტო შეტყობინებაზე პასუხის ავტომატური გენერაცია საშუალებას იძლევა დაცული იქნეს ელექტრონული ფოსტის ეთიკა და ოპერატიულად გაეცეს პასუხი მიღებულ შეტყობინებას ხანგრძლივად არყოფნის შემთხვევაშიც კი. ჩვეულებრივ, ყველა მიღებულ შეტყობინებაზე გაცივმა სტანდარტული პასუხი კავშირის დროებითი შეფერხების მიზეზის მითითებით. თუ ამ შემთხვევაში გამოყენებული იქნება ფილტრაციის ფუნქცია, შესაძლებელია შემაჯავალი შეტყობინებების კლასიფიკაცია გამგზავნის სახელის ან შეტყობინების თემის მიხედვით და შესაბამისად განსხვავებულ შეტყობინებებზე განსხვავებული ავტოპასუხების გენერაცია. ისინი ვინც ხანგრძლივად არ იმყოფებიან ადგილზე, ავტოპასუხის ფუნქციასთან ერთად იყენებენ ავტომატური გადამისამართების ფუნქციასაც. საყოველთაოდ მიღებული პრაქტიკაა Web-Mail-ის სამსახურის ერთერთ სერვერზე დროებითი „საფოსტო ყუთის“ შექმნა და მასზე იმ კორესპონდენციების გადამისამართება, რომელიც მიღებულია სააღრიცხვო ჩანაწერებით POP3 სერვერზე. ვინაიდან Web-ზე დაფუძნებულ ელექტრონულ ფოსტასთან მუშაობისათვის არ არის საჭირო არც საფოსტო კლიენტის არსებობა, არც მისი გამართვა, დროებით „საფოსტო ყუთთან“ მუშაობენ ჩვეულებრივი ბრაუზერით კავშირის ნებისმიერი ადგილიდან. სადაც არ უნდა იმყოფებოდეს

მომხმარებელი მას ყოველთვის აქვს საშუალება გადაათვალიეროს მიღებული ელექტრონული ფოსტა ერთერთ ხელმისაწვდომ Web-კვანძზე.

ექსპორტ-იმპორტის ფუნქციები. ფორმატები, რომლებშიც სხვადასხვა საფოსტო კლიენტები ინახავენ ელექტრონული ფოსტის შეტყობინებებს, შეიძლება განსხვავდებოდნენ. განსხვავებულია ასევე ლოგიკური ფოლდერების სტრუქტურა და შიდა სამისამართო წიგნების მონაცემთა ფორმატები. ელექტრონულ ფოსტასთან მუშაობის მძლავრი პროგრამები იძლევიან სხვა პროგრამების ფორმატში მონაცემების ექსპორტირების ან პირიქით, იმპორტირების საშუალებას.

ელექტრონული ფოსტის საშუალებების სპეციალური ფუნქციები.

საფოსტო საშუალებების სპეციალური ფუნქციები უპირველეს ყოვლისა უზრუნველყოფენ დიდი ინფორმაციული ნაკადების მომსახურებასთან დაკავშირებულ ოპერაციების ავტომატიზაციას და ძირითადად გამოიყენებიან ბიზნესში.

მასობრივი დაგზავნების ფუნქციები. ელექტრონული ფოსტის ჩვეულებრივი საშუალებები შესაძლებელს ხდიან გაიგზავნოს ერთი შეტყობინება რამოდენიმე მისამართზე ასლის (CC) ველში დამატებითი მისამართების მითითებით. ეს საკმარისი არ არის თუკი საჭიროა ათასობით საფოსტო გზავნილების გაგზავნა, ამასთან ყოველთვის სასურველი არ არის, რომ კლიენტმა გაიგოს სხვა ადრესატის მისამართები ამ ველის ჩანაწერების მიხედვით. ასეთ შემთხვევებში ხდება საფოსტო პროგრამის ინტეგრაცია დაგზავნის სიების სამსახურებთან..

დაგზავნის სიები არის ტექსტური ფაილი, რომელიც წარმოადგენს ჩვეულებრივ მონაცემთა ბაზას, რომელშიც ცალკეული ჩანაწერები გამოყოფილია სტანდარტულ გამყოფებით " : " ან ტაბულაციის სიმბოლოთი. შეტყობინებების დაგზავნა ხდება სიაში მოცემულ ყველა მისამართზე. პროგრამის დამატებითი საშუალებები ასევე შესაძლებელს ხდიან:

- ✓ მიღებული შეტყობინებების ანალიზის საფუძველზე ავტომატურად შეიტანოს დაგზავნის სიაში მისამართი (მაგალითად, კლიენტის თხოვნის მიხედვით ხელმოწერა საინფორმაციო ბიულეტენზე, ელექტრონულ კატალოგზე და ა.შ.);
- ✓ ავტომატურად ამოიღოს მისამართი დაგზავნის სიიდან (მაგალითად, კლიენტის თხოვნით მისი მისამართით რეკლამის გაგზავნის შეწყვეტის შემთხვევაში);
- ✓ დაჯგუფდეს დაგზავნის სიებში ჩანაწერები; მრავალი ფირმა უგზავნის ახალ კლიენტებს ერთი და იმავე შინაარსის წერილებს (ყურადღებისათვის მადლობას გადაგიხდით), ხოლო მუდმივ კლიენტებს სხვა შინაარსის წერილებს (ახალი წინადადებებით);
- ✓ მოძებნოს ერთნაირი ჩანაწერები დაგზავნის სიებში და გაანადგუროს;
- ✓ დაადგინოს და გააუქმოს არა აქტუალური ჩანაწერები (მაგალითად, ელექტრონული ფოსტის კლიენტის მისამართის შეცვლის შემთხვევაში).

საჭიროა განვასხვავოთ მასობრივი დაგზავნა და „საფოსტო დაბომბვა“. საფოსტო დაბომბვა არის მასობრივი დაგზავნების გზით მოუთხოვნელი კორესპონდენციებით „საფოსტო

ყუთის" გადავსების მიზანმიმართული, ბოროტული აქცია. ეს არის ინტერნეტის სარგებლობის წესების უხეში დარღვევა, რომელთა წინააღმდეგ სერვისის პროვაიდერს შეუძლია ადმინისტრაციული ზომების მიღება. ზოგიერთ შემთხვევაში, სისტემის ფუნქციონირების განზრახ დარღვევა შეიძლება დაკვალიფიცირდეს როგორც სამართლებრივი დანაშაული. ასეთ კვალიფიკაციას მიმართავენ თუკი შესაძლებელია პირდაპირი ზიანის არსებობის დამტკიცება.

მასობრივი დაგზავნა გამოირჩევა იმით, რომ შეტყობინებები იგზავნება სხვადასხვა მისამართზე. ის არ წარმოადგენს კანონდარღვევას, თუმცა ყოველთვის არ შეესაბამება სერვის-პროვაიდერთან დადებულ ხელშეკრულებას. ჩვეულებრივ პრაქტიკა ითვალისწინებს, რომ მასობრივი დაგზავნების წარმოებისათვის საჭიროა ხელშეკრულებაში შესაბამისი პუნქტის გათვალისწინება და ფინანსური მხარის განხილვა.

ლოკალური SMTP-სერვერის ფუნქციები. კორესპონდენციების მასობრივი დაგზავნა სერვისის მიმწოდებლის მიერ SMTP-სერვერის გამოყენებით დიდ დროს მოითხოვს, ვინაიდან სერვერზე იქმნება სხვადასხვა კლიენტისგან მიღებული შეტყობინებების რიგი. სპეციალურ შემთხვევებში იყენებენ საფოსტო სისტემებს, რომლებიც ითავსებენ საფოსტო კლიენტისა და SMTP-სერვერის ფუნქციებს. ისინი საშუალებას იძლევიან გაიგზავნოს კორესპონდენციები SMTP სერვერის გვერდის ავლით და უზრუნველყოფენ მაღალ წარმადობას (რამოდენიმე ათასი გზავნილი საათში).

პერსონალიზაციის ფუნქციები. მასობრივი დაგზავნისას მნიშვნელოვანია ცალკეული შეტყობინებების პერსონალიზაცია. იგი მდგომარეობს იმაში, რომ თითოეულ შეტყობინებას აქვს ინდივიდუალური ელემენტები, მაგალითად მიმართვა (ბატონო,

ქალბატონო, ბატონებო და ა.შ), ადრესატის სახელი და რაიმე პერსონალური ცნობები მის შესახებ. პერსონალიზაცია სრულდება საფოსტო პროგრამის მონაცემთა ბაზასთან და დაგზავნის სიებთან ურთიერთქმედების გზით. შეტყობინება მზადდება პაკეტის სახით, რომელსაც აქვს შერწყმის ველები.. მონაცემები შერწყმის ველებში ჩაისმება მონაცემთა ბაზიდან დაგზავნის სიებში მითითებული პარამეტრების შესაბამისად. პერსონალიზაციის ტექნოლოგიის წყალობით შესაძლებელი ხდება მნიშვნელოვნად გაიზარდოს სარეკლამო-მარკეტინგულ კომპანიებში გამოსმაურებები, კლიენტების ანკეტირების წარმოებისა და შემკვეთთან ნდობის დამყარებისათვის. მოცემულ მაგალითში, სურათზე 3,

პატივცემულო <ბატონო> <კიკვიძე>!

<21.04.00> თქვენ შეუკვეთეთ ჩვენს მაღაზიას წიგნი <ი. ჭავჭავაძე. ტომი 2>. ვიმედობნებით, იგი მიიღეთ დროულად და შესაძლებელად ჩათვლით შემდგომშიც ისარგებლოთ ჩვენი მომსახურებით.

გატყობინებთ, რომ დაწყებული <15.12.00>-დან გაყიდვაში იქნება ახალი წიგნი ანალოგიური თემატიკით <ი. ჭავჭავაძე ტომი 3>. როგორც მუდმივ კლიენტს, თქვენ მოგეცემათ დამატებითი შეღავათი <15> პროცენტი ფასდაკლებით. ვიღებთ შეკვეთებს.

დიდი პატივისცემით:

"სასარგებლო წიგნი"-ის სამსახური ადმინისტრაცია საინფორმაციო სამსახურის შეტყობინებები გაეგზავნება მხოლოდ იმ კლიენტებს, ვისაც სურთ რეგულარულად შეიტყონ გაყიდვაში მიღებული წიგნების შესახებ. თუ თქვენ გსურთ უარი თქვათ რეგულარული შეტყობინების მიღებაზე, გთხოვთ გამოგზავნოთ ჩვენს მისამართზე ნებისმიერი შეტყობინება თემით Unsubscribe.

სურ. 3 შეტყობინების პერსონალიზაცია შერწყმის ველების გამოყენებით

შერწყმის ველები ჩასმულია კუთხურ ფრჩხილებში. შეტყობინების მომზადებისას მონაცემები მათთვის მონაცემთა ბაზიდან აიღება.

დაშორებული ადმინისტრირების ფუნქციები. ზოგიერთ საფოსტო კლიენტს შეუძლია არა მხოლოდ გაუგზავნოს შეტყობინების სიგნალი დაშორებული კავშირის საშუალებებს, არამედ მიიღოს კიდევ მათგან მმართველი სიგნალები. საფოსტო სისტემების დაშორებული მართვა ხდება ტელეფონის აპარატების დახმარებით, რომელთაც აქვთ ნომრების ტონალური აკრეფის რეჟიმი. კავშირის დამყარების შემდეგ სისტემა აღიქვამს ციფრული ნაკრების სიგნალებს, როგორც ბრძანებებს. მსგავსი სისტემები საშუალებას იძლევიან გადაამისამართდეს მიღებული შეტყობინება ან ავტომატურად გაიგზავნოს წინასწარ მომზადებული პასუხის ერთ-ერთი ვარიანტი. შესაძლებელია ასევე ხმოვანი შეტყობინების გაგზავნა, რომელიც ნაკარნახევია დაშორებული სატელეფონო აპარატიდან.

ელექტრონული ფოსტის ეთიკა

ეტიკეტის მოთხოვნების მიხედვით ელექტრონულ ფოსტას უკავია შუალედური მდგომარეობა ჩვეულებრივი ფოსტასა და სატელეფონო კავშირს შორის. ეს მოთხოვნები უფრო მკაცრია, ვიდრე ჩვეულებრივი მიმოწერისას, მაგრამ არც ისე მკაცრი, როგორც სატელეფონო ურთიერთობისას. ელექტრონული ფოსტა შეიძლება განვიხილოთ როგორც „გადაღებული სატელეფონო ხარი“, ამიტომ არ არის აუცილებელი მიმართვის დროის გათვალისწინება.

ელექტრონული ფოსტის ეთიკის განხილვისას ცალ-ცალკე განიხილება სამსახურებრივი და პირადი მიმოწერა.

სამსახურებრივში იგულისხმება მიმოწერა ორგანიზაციებს შორის ან ორგანიზაციებსა და კერძო პირებს შორის.

სამსახურებრივი მიმოწერის ეთიკა.

✓ შეტყობინების მომზადებისას აუცილებელია სათაურის ყველა ველის შევსება. შეტყობინებაზე შეუვსებელი ველებით პასუხი შესაძლებელია არ მოვიდეს, ვინაიდან ავტომატური ფილტრაციის საშუალებებს შეუძლიათ არ დაუშვან მიღებული შეტყობინება ადრესატამდე.

✓ შეტყობინების შინაარსი (ტანი) უნდა იყოს მოკლე. მასში უნდა იყოს აღწერილი მიმართვის მიზეზები და მკაფიოდ გამოხატული კონკრეტული თხოვნა (მოთხოვნა). სწორედ თხოვნა (მოთხოვნა) წარმოადგენს გადაწყვეტილების მიღების საფუძველს საპასუხო შეტყობინების შესრულებისათვის. მოთხოვნის მკაფიოდ ფორმულირების გარეშე პასუხი არ არის გარანტირებული.

✓ ელექტრონული ფოსტის შეტყობინებაში გამოხატული თხოვნა ან მოთხოვნა, არ უნდა მოითხოვდეს ადრესატისაგან ელექტრონული ფოსტის გარდა სხვა კავშირის საშუალებების გამოყენებას. როგორც წესი, უპასუხოდ რჩება რომელიმე Web-კვანძზე სტუმრობის, ფაქსის გაგზავნის ან მითითებულ ნომერზე ტელეფონით დარეკვის შესახებ თხოვნით მიმართვა.

✓ ელექტრონული ფოსტის შეტყობინებებზე პასუხის ვადაა 24 საათი. პასუხის შინაარსი უნდა შეესაბამებოდეს მოთხოვნის შინაარსს. თუ სრულფასოვანი პასუხის გაცემა ამ დროში არ ხერხდება, საჭიროა გაიცეს ფორმალური პასუხი გადაწყვეტილების მიღების მოსალოდნელი ვადის მითითებით.

✓ პასუხის მიუღებლობის შემთხვევაში საჭიროა შემოწმდეს სწორად იყო თუ არა დაცული შეტყობინებაზე ფორმალური მოთხოვნები (კვლევის შევსება, მოსალოდნელი რეაქციის მკაფიო მითითება, შეტყობინების ავტორის ხელმოწერა). სამსახურებრივი მიმოწერისას განმეორებითი მიმართვები დასაშვებია მხოლოდ დროის გარკვეული ინტერვალის შემდეგ, არა ნაკლები ერთი კვირისა (თუ გარემოებები საშუალებას იძლევა უკეთესია შეტყობინებებს შორის ორკვირიანი ინტერვალის დაცვა). უფრო ხშირი მიმართვები განხილულ იქნას როგორც სპამ-ი, რის შემდეგაც მიმართვის წყაროს ბლოკირება მოხდება ფილტრაციის საშუალებებით.

✓ სამსახურებრივ მიმოწერაში ფაილების გადასაგზავნად საფოსტო ჩაღაგებების მექანიზმის გამოყენება დასაშვებია მხოლოდ პარტნიორის პირდაპირი თხოვნით. არ უნდა მოხდეს არავითარი საფოსტო ჩაღაგებების გაგზავნა საკუთარი ინიციატივით.

✓ ელექტრონული ფოსტით ჩაღაგებული ფაილით მოუთხოვნელი შეტყობინების მიღების შემთხვევაში, საფოსტო ჩაღაგებები უნდა განადგურდეს გაუხსნელად, წაუკითხავად. ბევრი საფოსტო კლიენტის სუსტი მხარე დაკავშირებულია საფოსტო ჩაღაგებების არაკორექტულ დამუშავებასთან. ასეთ სისუსტეებს ხშირად იყენებენ ბოროტმზრახველები კომპიუტერული სისტემების ფუნქციონირების დარღვევის მიზნით.

✓ თუ საფოსტო ჩაღაგებების გაგზავნა შეთანხმებულია ორივე მხარის მიერ, საჭიროა შეფასდეს გადასაგზავნი ფაილის ზომა. დასაშვებად ითვლება ზომა 100 კ.ბაიტამდე. თუ რეალური ზომა მეტია, საჭიროა ამის შესახებ წინასწარ ეცნობოს

პარტნიორს (კავშირის ნებისმიერი საშუალების გამოყენებით). წინასწარი გაფრთხილების აუცილებლობა დაკავშირებულია იმასთან, რომ ადრესატის საფოსტო კლიენტი შეიძლება მომართული იყოს დიდი ზომის ჩალაგებების მქონე შეტყობინებების დაბლოკვაზე. ზოგიერთი საფოსტო პროგრამა საშუალებას იძლევა „დაიჭრას“ გრძელი საფოსტო ჩალაგებები მოკლე ფრაგმენტებად, რომლებიც რამდენიმე ჯერზე გადაიგზავნება. ამ შემთხვევაში წინასწარაა საჭიროა იმაში დარწმუნება, რომ ადრესატის საფოსტო კლიენტს (საფოსტო პროგრამას) შეუძლია მათი სწორად აწყობა.

პირადი მიმოწერის ეთიკა.

✓ შეტყობინების მომზადებისას აუცილებელია სათაურის ყველა ველის შევსება. შეტყობინებაზე შეუვსებელი ველებით პასუხი შეიძლება არ მოვიდეს ზემოთ აღნიშნული მიზეზების გამო.

✓ არამართებულია უცნობ პირებთან მიმართვა, რომლებიც არ აქვეყნებენ თავის მისამართს ქსელში ან მასობრივი ინფორმაციის საშუალებებში. უკიდურესი აუცილებლობის შემთხვევაში საჭიროა შეტყობინების პირველ სტრიქონებში წარდგენა და ახსნა თუ საიდან გახდა ცნობილი მისამართი.

✓ პირად მიმართვაზე პასუხის ვადა არ არის რეგლამენტირებული. მისი დადგენა ხდება ორ პარტნიორს შორის ურთიერთობის არსებული პრაქტიკით. თუ ასეთი პრაქტიკა არ არსებობს (პირველი მიმართვისას), პასუხი უნდა გაეცეს 24 საათის განმავლობაში.

✓ პასუხის მომზადებისას საჭიროა გამოყენებულ იქნას ორიგინალური შეტყობინების ენა და კოდირების სიმბოლოები.

✓ უცნობი პირისათვის გაგზავნილ შეტყობინებაზე პასუხის მიუღებლობის შემთხვევაში განმეორებითი მიმართვა დაუშვებელია და განიხილება როგორც სპამი.

✓ უცნობი წყაროდან მოუთხოვნილი შეტყობინების მიღების შემთხვევაში არ არის რეკომენდირებული პასუხის გაცემა მიმართვის შეწყვეტის თხოვნითაც კი. ინტერნეტში არის სამსახურები, რომლებიც ახდენენ ელექტრონული ფოსტის მისამართების შეგროვებას სარეკლამო კომპანიებისათვის მიყიდვის მიზნით. კლიენტისაგან ნებისმიერი პასუხის მიღების ფაქტი ამტკიცებს მისამართის არსებობას, მნიშვნელოვნად ამაღლებს მის კომერციულ ფასეულობას სარეკლამო სამსახურებისათვის, ხელს უწყობს მისამართის ახალ გადაყიდვას და შესაბამისად, მხოლოდ ზრდის არასასურველი შეტყობინებების მოცულობას.

✓ ჩალაგებული ფაილების მქონე მოუთხოვნილი შეტყობინებების მიღებისას ისინი გაუსხნელად უნდა განადგურდეს. ეს მოთხოვნა კატეგორიულია, იგი ვრცელდება ისეთ ფაილებზეც კი რომლებიც მიღებულია ახლობელი ადამიანებისაგან, მეგობრებისა და ნაცნობებისაგან.

✓ ჩალაგებული ფაილის გაგზავნის აუცილებლობის შემთხვევაში საჭიროა წინასწარ პარტნიორის გაფრთხილება ცალკე შეტყობინებებით, წინააღმდეგ შემთხვევაში ეს ფაილი განადგურდება. თუ ჩალაგებული ფაილი დიდი ზომისაა (100 კბაიტზე მეტი), საჭიროა არა მხოლოდ ადრესატის წინასწარ გაფრთხილება, არამედ მისი თანხმობის მიღება - გადაგზავნაზე.

ელექტრონული ფოსტის შეთანხმებები.

სამსახურებრივი მიმოწერისათვის გამოიყენება ის ენა და სიმბოლოების კოდირების ის მეთოდი, რომელიც დამტკიცებულია მოცემულ ორგანიზაციაში, იმისგან დამოუკიდებლად თუ რომელ ენაზე და რომელი კოდირებით მიიღება შეტყობინებები კორესპონდენტისაგან. გაურკვეველობის შემთხვევაში საჭიროა მიმართვა უფლებამოსილ პირზე, მაგალითად სისტემურ ადმინისტრატორზე.

პირადი მიმოწერისას საპასუხო შეტყობინებების მომზადებისას საჭიროა იმავე ენისა და კოდირების მეთოდის გამოყენება, რომელიც გამოყენებულია საწყის შეტყობინებაში.

ელექტრონული ფოსტის შეტყობინებების მომზადებისას გამოიყენება ეგრეთ წოდებული *ემოტიკონები* და *აბრევიატურები*. ემოტიკონი არის ავტორის ემოციების გადმოსაცემად განკუთვნილი სიმბოლოების კომბინაცია. აბრევიატურა არის საყოველთაოდ მიღებული სიტყვის შემოკლება, რომელიც გამოიყენება კლავიატურიდან ინფორმაციის შეტანის გამარტივებისათვის. როგორც წესი, ემოტიკონებისა და აბრევიატურების გამოყენება შემოიფარგლება პირადი მიმოწერით. სამსახურებრივ მიმოწერაში მათი გამოყენება არასასურველია. ემოტიკონებს ქმნიან სიმბოლოების კლავიატურული კომბინაციის გამოყენებით. გამოსახულებები უნდა აღვიქვათ წარმოსახვით 90°-ით მობრუნებული საათის ისრის მიმართულებით.

მაგ: :-)-ღიმილი; :-/ ირონია; :-(- დარდი; და სხვა

შესაძლო ემოტიკონების რაოდენობა ასეულობით იზომება. მათი გამოყენება შესაძლებელს ხდის გამოცოცხლდეს არაფორმალური მიმოწერა, მაგრამ ამასთან საჭიროა ზომიერების

დაცვა. ემოტიკონების დანიშნულებაა მარტივი და გასაგები გრძნობების გადაცემა და არა პარტნიორის დაყენება გამოცანის წინაშე.

ყველაზე ფართოდ გამოყენებული აბრევიატურებიდან კი უნდა ავნიშნოთ შემდეგი:

BTW - by the way - სხვათაშორის.....

IMNO - in my humble opinion - ჩემი მოკრძალებული აზრით.....

AFAIK - as for as I know - რამდენადაც ჩემთვის ცნობილია.....

FYEO - for you eyes only - მკაცრად ჩვენს შორის.....

FYI - for your information - ცნობისათვის.....

აბრევიატურები განსაკუთრებით ხშირად გამოიყენება ახალი ამბების ჯგუფზე მიმართული ელექტრონული ფოსტის შეტყობინებებში (ტელეკომფერენციები). ჩვეულებრივ მათ იყენებენ მხოლოდ მაშინ, როცა პარტნიორთან ელექტრონული ურთიერთობების პრაქტიკა უკვე ჩამოყალიბებულია.

ელექტრონული ფოსტის უსაფრთხოება.

უსაფრთხოების თვალსაზრისით, ელექტრონულ ფოსტასთან მუშაობისას არსებობს შემდეგი სახის საშიშროებები:

- ✓ კონფიდენციალური ინფორმაციის გაჟონვა;
- ✓ მომსახურებაზე უარის თქმა;
- ✓ კომპიუტერული ვირუსით დაზიანება;
- ✓ კომპიუტერში აქტიური შემადგენლობის შეღწევა.

კონფიდენციალური ინფორმაციის გაჟონვის თავიდან აცილების მიზნით საფოსტო გაცვლებისას იყენებენ სიმეტრიული და არასიმეტრიული კრიპტოგრაფიის მეთოდებს. სიმეტრიული

კრიპტოგრაფის დროს ორივე მხარე იყენებს დაშიფვრისა და გაშიფვრის ერთნაირ პროგრამულ უზრუნველყოფას. არჩეული გასაღებით (პაროლი) შეტყობინების დაშიფვრისას გამგზავნი ატყობინებს ადრესატს გასაღებს კავშირის ალტერნატიული საშუალებების, მაგალითად ტელეფონის გამოყენებით. არასიმეტრიული დაშიფვრის დროს შეტყობინებას გამგზავნი დაშიფრავს მიმღების სერთიპიკატის დახმარებით (ღია გასაღები). თანამედროვე საფოსტო კლიენტების უმრავლესობა ავტომატურად ასრულებს ამ ოპერაციებს, როგორც გამგზავნისათვის, ისე ადრესატისათვის შეუმჩნეველად.

„მომსახურებაზე უარის თქმად“ წოდებული საშიშროება დაკავშირებულია ადრესატის საფოსტო სერვერების წყობილებიდან მიზანმიმართულ გამოსვლასთან, მაგალითად შეტყობინებებით ფოსტის გადავსებასთან. საწინააღმდეგო ზომად იყენებენ ჯერ ერთი, ისეთ საფოსტო კლიენტებს, რომელთაც შეუძლიათ სერვერზე მიღებული შეტყობინების გაანალიზება მომხმარებლის კომპიუტერში ჩატვირთვამდე და მეორე, „საფოსტო ყუთის“ გადავსების თავიდან ასაცილებლად საჭირო არ არის საკუთარი ელექტრონული ფოსტის მისამართის ფართოდ აფიშირება. თუ კი აუცილებელია მისამართის გამოქვეყნება, Web-Mail-ის ერთერთ უფასო სამსახურში ხსნიან საადრიცხვო ჩანაწერს და დროებით მას იყენებენ. საკუთარი მისამართის ქსელში გაგზავნისას საჭიროა იმის მხედველობაში მიღება, რომ არსებობენ ავტომატური პროგრამული საშუალებები რომელთაც შეუძლიათ ნებისმიერი ტიპის ფაილის დათვალიერება მათში E-Mail-ის მისამართების მოძებნის მიზნით. ჩვეულებრივ ეს საშუალებები ღოკუმენტში ეძებენ „@“ სიმბოლოს, ამიტომ მას ცვლიან რაიმე სხვა

სიმბოლოთი, რომელიც გასაგებია ადამიანისათვის, მაგრამ არა პროგრამისათვის, მაგალითად ასე:

myname@absd.com-ის ნაცვლად იყენებენ: myname#absd.com უფრო საიმედოა მეთოდი, როცა ადრესატის სახელის ნაცვლად გამოიყენება სტანდარტული შაბლონი, მაგალითად NOSPAM, ნაცვლად: myname@absd.com იყენებენ: nospammyname#absd.com იმას რომ თავსართი „nospam“ უნდა ჩამოცილდეს, მომხმარებელი თავად უნდა მიხედეს.

ელექტრონული ფოსტის საშუალებით შესაძლებელია როგორც „კლასიკური“ კომპიუტერული ისე სპეციალური „საფოსტო“ ვირუსების მიღება. კლასიკური ვირუსები ვრცელდება შესრულებადი ფაილების (პროგრამები) სახით, რომლებიც ჩალაგებულია ელექტრონული ფოსტის შეტყობინებაში. ასეთი მეთოდით შეიძლება დაზიანდეს ნებისმიერი კომპიუტერული სისტემა, გამოყენებული საფოსტო კლიენტისაგან დამოუკიდებლად. ელექტრონული ფოსტის შეტყობინებებთან ერთად მიღებული ყველა შესრულებადი ფაილი პოტენციურად საშიშია, მაშინაც კი, თუ ისინი მიღებულია ნაცნობებისაგან. საჭიროა გვახსოვდეს, რომ ელექტრონული ფოსტა არასასურველი საშუალებაა პროგრამების გაცვლისათვის. თუ აუცილებელია ვინმესთან სასარგებლო პროგრამის გაზიარება, საჭიროა არა თვით პროგრამის გაგზავნა, არამედ ცნობების მიწოდება იმის შესახებ თუ სად შეიძლება მისი მოპოვება. შედარებით სასარგებლო და შემოწმებული სამსახურებრივი პროგრამები ქსელში უნდა იყოს გამოქვეყნებული. ამ შემთხვევაში წერილის ტექსტში საკმარისია მოყვანილი იქნას მისი URL-მისამარი

„საფოსტო ვირუსების“ მუშაობის მექანიზმი ემყარება ცალკეულ საფოსტო პროგრამებში არსებული "სისუსტეების" გამოყენებას. შედარებით ხშირად ვირუსულ თავდასხმას განიცდიან სტანდარტული პროგრამული უზრუნველყოფის მომხმარებლები, კერძოდ პროგრამის Outlook Explorer. „საფოსტო ვირუსის“ ამოქმედებისათვის არცაა საჭირო იმ ფაილის შესრულება, რომელიც საფოსტო ჩაღაგების სახითაა მიღებული, საკმარისია მისი მხოლოდ გახსნა. სწორედ ამიტომ, ელექტრონული ფოსტის ეთიკის განხილვისას აღნიშნული იყო, რომ არაა რეკომენდირებული საფოსტო ჩაღაგებების გაგზავნა მიმღების წინასწარ გაფრთხილების გარეშე. ხოლო ჩაღაგებული ფაილების მქონე შეტყობინებების მოულოდნელი მიღებისას საჭიროა მისი განადგურება დათვალიერების გარეშე.

თავი 4. კომპიუტერული უსაფრთხოება

4.1 კომპიუტერული უსაფრთხოების ცნება.

უსაფრთხოების ცნება გამოთვლით ტექნიკაში გულისხმობს კომპიუტერის საიმედო მუშაობას, მნიშვნელოვანი მონაცემების საიმედო შენახვას, უფლების არ მქონე პირების მიერ ცვლილებების შეტანისაგან ინფორმაციის დაცვას, ელექტრონული კავშირით მიმღწერის საიდუმლოების დაცვას და სხვა. რა თქმა უნდა, ყოველ ცივილიზებულ ქვეყანაში მოქალაქეების უსაფრთხოებას კანონი იცავს, მაგრამ გამოთვლითი ტექნიკის სფეროში საკანონმდებლო პრაქტიკა სუსტადაა განვითარებული, ხოლო კანონშემოქმედებითი პროცესი ვერ უსწრებს ტექნოლოგიების განვითარებას, ამიტომ კომპიუტერული სისტემების მუშაობის საიმედოობა ძირითადად თვითდაცვის ზომებზეა დამყარებული. კომპიუტერისათვის მთავარ საფრთხეს ე.წ. პროგრამა-ვირუსები წარმოადგენენ.

კომპიუტერული ვირუსები.

კომპიუტერული ვირუსი არის სხვა პროგრამაში ან დოკუმენტში, ან მონაცემების მატარებლების განსაზღვრულ არეებში ჩართული პროგრამული კოდი, რომელიც ასრულებს არასანქცირებულ მოქმედებებს მის მატარებელ კომპიუტერზე.

კომპიუტერული ვირუსებების ძირითად ტიპებს წარმოადგენენ:

- ✓ პროგრამული ვირუსები;
- ✓ ჩამტვირთავი ვირუსები;
- ✓ მაკროვირუსები.

პროგრამული ვირუსები.

პროგრამული ვირუსები არის გამოყენებით პროგრამებში მიზნობრივად ჩანერგილი პროგრამული კოდის ბლოკები. დავირუსებული პროგრამების ამუშავებისას ხდება მასში ჩადებული ვირუსული კოდის ამუშავება. ამ კოდის მუშაობა იწვევს მომხმარებლისაგან შეუმჩნეველ ცვლილებებს ხისტი დისკების ფაილების სისტემაში ან/და სხვა პროგრამების შინაარსში. მაგალითად, ვირუსულ კოდს შეუძლია სხვა პროგრამების „სხეულში“ თვითწარმოქმნა. ამ პროცესს გამრავლებას უწოდებენ. გარკვეული დროის გასვლის შემდეგ, შექმნის რა საკმარისი რაოდენობის ასლს, პროგრამული ვირუსი გადადის დამანგრეველ მოქმედებაზე: პროგრამისა და ოპერაციული სისტემის მუშაობის დარღვევაზე, ხისტ დისკზე შენახული ინფორმაციის განადგურებაზე და სხვა. ამ პროცესს *ვირუსულ შეტევას* უწოდებენ.

ყველაზე დამანგრეველ ვირუსებს შეუძლიათ გამოიწვიონ ხისტი დისკის გადაფორმატება. ვინაიდან დისკის გადაფორმატება საკმარისად ხანგრძლივი პროცესია, რომელიც ვერ შესრულდება მომხმარებლის შეუმჩნეველად, ამიტომ ხშირ შემთხვევაში, პროგრამული ვირუსები ხისტი დისკის სისტემურ სექტორებში მონაცემების განადგურებით შემოიფარგლებიან, რაც ფაილების სისტემის დაკარგვის ტოლფასია. ასეთ შემთხვევაში ხისტი დისკის მონაცემები ხელუხლებელია, მაგრამ მათი გამოყენება სპეციალური საშუალებების გარეშე შეუძლებელია, ვინაიდან უცნობია დისკის რომელი სექტორი რომელ ფაილს ეკუთვნის. მონაცემების აღდგენა ამ შემთხვევაში თეორიულად შესაძლებელია, მაგრამ ამ სამუშაოების შრომატევადობა ძალზე მაღალია.

ითვლება, რომ არც ერთ ვირუსს არ შეუძლია მწყობრიდან გამოიყვანოს კომპიუტერის აპარატული საშუალებები. მაგრამ, არის შემთხვევები, როდესაც კომპიუტერის აპარატული და პროგრამული უზრუნველყოფა იმდენადაა ერთმანეთთან დაკავშირებული, რომ პროგრამული დაზიანების აღმოფხვრა მხოლოდ აპარატული საშუალებების შეცვლით ხერხდება. ასე მაგალითად, უმრავლეს თანამედროვე დედა პლატაში შეტანა-გამოტანის საბაზო სისტემა (*BIOS*) ინახება მუდმივ მეხსიერების მოწყობილობაში (ე.წ. *ფლეშ-მეხსიერება*). ზოგიერთი პროგრამული ვირუსები *BIOS*-ის მონაცემების გასანადგურებლად იყენებენ სწორად ფლეშ-მეხსიერების მიკროსქემაში ინფორმაციის გადაწერის შესაძლებლობას. ასეთ შემთხვევაში კომპიუტერის მუშაობის უნარიანობის აღსადგენად საჭიროა ან იმ მიკროსქემების შეცვლა, რომელშიც შენახულია *BIOS*, ან მისი გადაპროგრამება სპეციალური პროგრამული საშუალებებით.

პროგრამული ვირუსები კომპიუტერში ვრცელდებიან შეუმოწმებელი გარე მატარებლების გამოყენებით (დისკეტები, კომპაქტდისკები და ა.შ) ან ინტერნეტიდან მიღებული პროგრამების გაშვებით. განსაკუთრებული ყურადღება უნდა მიექცეს სიტყვას „გაშვებით“, ჩვეულებრივად დავირუსებული ფაილების ასლის გაკეთებისას კომპიუტერი არ შეიძლება დავირუსდეს. ამიტომ, ინტერნეტით მიღებული ყველა ფაილი უნდა შემოწმდეს უსაფრთხოებაზე, ხოლო თუ მიღებულია მოუთხოვნელი მონაცემები უცნობი წყაროდან, იგი უნდა განადგურდეს დაუთვალე-რებლად. ვირუსული პროგრამების გავრცელების ჩვეულებრივი ხერხია ელექტრონული წერილი „რეკომენდაციით“ ამოვიღოთ და გავუშვათ თითქოსდა სასარგებლო პროგრამა.

ჩამტვირთავი ვირუსები.

ჩამტვირთავი ვირუსები პროგრამული ვირუსებისაგან გავრცელების მეთოდით განსხვავდებიან. ისინი აზიანებენ არა პროგრამულ ფაილებს, არამედ, დისკური მექსიერების განსაზღვრულ სისტემურ არეებს. ამას გარდა ჩართულ კომპიუტერში მათ შეუძლიათ დროებით განთავსდნენ ოპერატიულ მექსიერებაშიც.

ჩვეულებრივად დავირუსება ხდება კომპიუტერის ჩატვირთვის მცდელობისას ისეთი დისკური მატარებლებიდან, რომლის სისტემური არე შეიცავს ჩამტვირთავ ვირუსს. მაგალითად, კომპიუტერის მოქნილი მაგნიტური დისკიდან ჩატვირთვისას, თავდაპირველად ვირუსი შეაღწევს ოპერატიულ მექსიერებაში, ხოლო შემდეგ ხისტი დისკის ჩამტვირთავ სექტორში. შემდეგში, ეს კომპიუტერი თავად ხდება ვირუსის გავრცელების წყარო.

მაკროვირუსები.

ეს ვირუსების განსაკუთრებული კატეგორიაა, რომლებიც აზიანებენ ისეთ დოკუმენტებს, რომლებიც შესრულებულია იმ პროგრამებში რომლებსაც აქვთ, ეგრეთწოდებული, მაკრობრძანებების შესრულების საშუალებები. კერძოდ, ასეთ დოკუმენტებს მიეკუთვნებიან ტექსტური პროცესორის Microsoft Word დოკუმენტები (მათ .doc გაფართოება აქვთ). დავირუსება ხდება დოკუმენტის გახსნისას პროგრამის ფანჯარაში თუ კი მასში გამორთული არ არის მაკრობრძანებების შესრულების შესაძლებლობა. ისე, როგორც სხვა ტიპის ვირუსების, ამ ვირუსის შემოტევის შედეგი შეიძლება იყოს როგორც შედარებით უწყინარი ასევე დამანგრეველიც.

4.2 კომპიუტერული ვირუსებისაგან დაცვის მეთოდები.

კომპიუტერული ვირუსებიდან დაცვის სამი ხერხი არსებობს.

- ✓ ვირუსების შემოტანის აცილება;
- ✓ ვირუსების შემოტევის აცილება, თუ კი ვირუსი მაინც შემოვიდა;
- ✓ დამანგრეველი შედეგების აცილება, თუ კი შემოტევა მაინც მოხდა,

შესაბამისად დაცვის რეალიზაციის სამი მეთოდი არსებობს:

- ✓ დაცვის პროგრამული მეთოდები;
- ✓ დაცვის აპარატული მეთოდები;
- ✓ დაცვის ორგანიზაციული მეთოდები.

მნიშვნელოვანი ინფორმაციის დაცვის საკითხში ხშირად იყენებენ ყოფით მიდგომას: „ავადმყოფობა უკეთესია ავიცილით, ვიდრე ვუშკურნალოთ“. სამწუხაროდ სწორედ ეს იწვევს უმეტესად დამანგრეველ შედეგებს. შევქმნით რა ბასტიონებს კომპიუტერში ვირუსების შეღწევის გზაზე, არ შეიძლება დავეყრდნოთ მათ და დავრჩეთ მათი დამანგრეველი შეტევის შემდეგ მოქმედებისათვის მოუმზადებელნი. ამასთან ერთად, ვირუსული შეტევა არ არის მნიშვნელოვანი მონაცემების დაკარგვის ერთადერთი და ყველაზე გავრცელებული მიზეზი. არსებობენ პროგრამული ჩავარდნები, რომელსაც შეუძლია გამოიყვანონ მწყობრიდან ოპერაციული სისტემა, აგრეთვე აპარატული ჩავარდნები, რომელსაც შეუძლია გახადოს ხისტი დისკი მუშაობის უუნარო. ყოველთვის არსებობს კომპიუტერის დაკარგვის ალბათობა მონაცემებთან ერთად, მოპარვის, ხანძრის ან სხვა სტიქიური უბედურების გამო.

ამიტომ უსაფრთხოების სისტემის შექმნა პირველ რიგში საჭიროა დაიწყოს „ბოლოდან“ - ნებისმიერი მოქმედებით გამოწვეული დამანგრეველი შედეგების თავიდან აცილებით, იქნება ეს ვირუსული შეტევა, გაქურდვა თუ ხისტი დისკის მწყობრიდან გამოსვლა. მონაცემებთან საიმელო და უსაფრთხო მუშაობა მიიღწევა მხოლოდ მაშინ, როდესაც ნებისმიერი მოულოდნელი მოვლენა, მათ შორის კომპიუტერის სრული ფიზიკური განადგურება არ გამოიწვევს კატასტროფულ შედეგებს.

ანტივირუსული დაცვის საშუალებები ინფორმაციის დაცვის ძირითად საშუალებას წარმოადგენს მნიშვნელოვანი მონაცემების სათადარიგო ასლების გაკეთება. ზემოთ ჩამოთვლილი მიზეზებით ინფორმაციის დაკარგვის შემთხვევაში ხისტ დისკებს გადააფორმატებენ და ხელახალი ექსპლოატაციისათვის ამზადებენ. „სუფთა“ დაფორმატებულ დისკზე აყენებენ დისტრიბუტულ კომპაქტდისკიდან ოპერაციულ სისტემას, შემდეგ ასევე დისტრიბურული მატარებლიდან აყენებენ ყველა აუცილებელ პროგრამულ უზრუნველყოფას. კომპიუტერის აღდგენა მთავრდება სათადარიგო ასლებიდან მონაცემების აღდგენით.

მონაცემების რეზერვირებისას მხედველობაში უნდა გვქონდეს ის, რომ ინტერნეტის ქსელის სამსახურებთან მიმართვის ყველა სარეგისტრაციო და პაროლის მონაცემები ცალკე უნდა შეინახოს. მიზანშეწონილი არაა მათი კომპიუტერებზე შენახვა. ჩვეულებრივად შენახვის ადგილია სამსახურებრივი დღიური განყოფილების ხელმძღვანელის სეიფში.

სათადარიგო ასლების შექმნის ღონისძიებების შედგენისას აუცილებელია გავითვალისწინოთ, რომ სათადარიგო ასლები ინახებოდეს კომპიუტერისაგან დამოუკიდებლად. მაგალითად, იგი-

ვე კომპიუტერის სხვა ხისტ დისკზე სათადარიგო ასლის შენახვა მხოლოდ უსაფრთხოების ილუზიას ქმნის. შედარებით ახალს და საკმარისად სამიწლო ხერხს მნიშვნელოვანი და არა კომფიდენციალური მონაცემების შესანახად წარმოადგენს დაშორებული სერვერების Web-პაპკაში ინტერნეტში მათი შენახვა. არის სამსახურები, რომლებიც უფასოდ სთავაზობენ მომხმარებელს რამოდენიმე მეგაბაიტამდე სივრცეს მონაცემების შესანახად.

კომფიდენციალური მონაცემების სათადარიგო პირებს ინახავენ გარე მატარებლებზე, რომლებსაც ინახავენ სეიფში, სასურველია სხვა შენობაში. სათადარიგო პირების მომზადების საორგანიზაციო გეგმის დამუშავებისას ითვალისწინებენ არანაკლებ ორი სათადარიგო პირის შექმნას სხვადასხვა ადგილზე შენახვით. მათ შორის ასრულებენ როტაციას. მაგალითად, კვირის განმავლობაში ყოველდღე გადააქვთ მონაცემების ასლები სათადარიგო კომპლექტზე „A“, ხოლო ერთი კვირის შემდეგ მათ ცვლიან კომპლექტით „B“ და ა.შ.

ინფორმაციის დაცვის დამხმარე საშუალებას წარმოადგენს ანტივირუსული პროგრამები და დაცვის აპარატული საშუალებები. მაგალითად, მთავარ პლატაზე გადამრთველის უბრალო ამორთვა არ მისცემს მუდმივი მეხსიერების პროგრამირებული მიკროსქემის წაშლის საშუალებას, იმის მიუხედავად თუ ვინ შეეცდება ამის გაკეთებას: კომპიუტერული ვირუსი, ბოროტი თუ არასწორი მომხმარებელი.

არსებობენ საკმარისად ბევრი ანტივირუსული დაცვის პროგრამები. ისინი იძლევიან შემდეგ შესაძლებლობებს:

1. გარე მატარებლებზე (მაგ. მოქნილ დისკზე) ხისტი დისკის „სახის“ შექმნა. ხისტი დისკის სისტემური არის

მონაცემების დაზიანებისას დისკის შენახული „სახე“ იძლევა თუ ყველა მონაცემების არა უმეტესი ნაწილის აღდგენის საშუალებას. ამ საშუალებით შეიძლება დაიცვათ მონაცემების დაკარგვა აპარატული ჩავარდნებისას და ხისტი დისკის არასწორი დაფორმატებისას.

2. ხისტი დისკების რეგულარული სკანირება ვირუსებზე ჩვეულებრივად, ავრომატურად სრულდება კომპიუტერის ყოველი ჩართვისას და გარე მატარებლების წამკითხავ მოწყობილობაში ყოველი ჩადებისას. სკანირებისას მხედველობაში მისაღებია ის, რომ ანტივირუსული პროგრამა ვირუსს ეძებს პროგრამის კოდისა და მონაცემთა ბაზაში არსებული მისთვის ცნობილი ვირუსების კოდების შედარებით. თუ მონაცემთა ბაზა მოძველებულია, ხოლო ვირუსი ახალი, პროგრამის სკანირება მას ვერ აღმოაჩენს. საიმედო მუშაობისათვის საჭიროა ანტივირუსული პროგრამების განახლება. განახლების სასურველი პერიოდია ორ კვირაში ერთხელ; დასაშვებია სამ თვეში ერთხელ. მაგალითისათვის, დამანგრეველი შედეგები ვირუსის W95.CIH.1075 (ჩერნობილი), რომელმაც 1999 წლის 26 აპრილს გამოიწვია ასი ათასობით კომპიუტერზე ინფორმაციის განადგურება იყო არა მისგან თავდაცვის უქონლობა, არამედ ამ საშუალებების (ანტივირუსული ბაზის) განახლების დაყოვნება.
3. ფაილის ზომებისა და სხვა ატრიბუტების შემოწმება. რამდენადაც ზოგიერთი კომპიუტერული ვირუსები გამრავლების ეტაპზე ცვლიან დავირუსებული ფაილების ზომებს, მაკონტროლებელი პროგრამები აღმოაჩენენ მათ მოქმედებას და აფრთხილებენ მომხმარებელს.

4. ხისტ დისკთან მიმართვის კონტროლი. რამდენადაც, კომპიუტერული ვირუსების საშიში ოპერაციები ასე თუ ისე მიმართულია ხისტ დისკზე ჩაწერილი მონაცემების მოდიფიკაციისაკენ, ანტივირუსულ პროგრამებს შეუძლიათ აკონტროლონ მასთან მიმართვები და გააფრთხილონ მომხმარებელი საეჭვო აქტივობის შემთხვევაში.

4.3 ინფორმაციის დაცვა ინტერნეტში.

ინტერნეტში მუშაობისას მხედველობაში უნდა ვიქონიოთ ის, რომ რამდენადაც საერთაშორისო ქსელი ღიაა თვითოეული კლიენტისათვის, იმდენად მისი კომპიუტერული სისტემის რესურსები გარკვეულ პირობებში ღიაა ყველასათვის ვინც ფლობს ამის აუცილებელ საშუალებას.

კერძო მომხმარებლისათვის ეს ფაქტი განსაკუთრებულ როლს არ თამაშობს, მაგრამ ამის ცოდნა აუცილებელია, რომ არ დავეშვათ იმ ქვეყნების კანონმდებლობის დამრღვევი მოქმედებები, რომელთა ტერიტორიაზეცაა განლაგებული ინტერნეტის სერვერები. ასეთ მოქმედებებს განეკუთვნებიან კომპიუტერული სისტემის მუშაობის უნარიანობის დარღვევის განზრახული ან უნებლიე ცდები. დაცული სისტემების „გატეხვა“, ისეთი პროგრამების გამოყენება და გავრცელება, რომლებიც არღვევენ კომპიუტერული სისტემების მუშაობის უნარიანობას (ნაწილობრივ, კომპიუტერული ვირუსები). საერთაშორისო ქსელში მუშაობისას უნდა გვახსოვდეს, რომ აბსოლუტურად ყველა მოქმედება ფიქსირდება და აღირიცხება სპეციალური პროგრამული საშუალებებით და ინფორმაცია, როგორც კანონიერი ისე უკანონო მოქმედებაზე სადაც აუცილებლად გროვდება. ამგვარად, ინტერნეტში ინფორმა-

ციის გაცვლას უნდა მივუდგეთ, როგორც მიმოწერას, ჩვეულებრივი საფოსტო ღია ბარათების გამოყენებით. ინფორმაცია თავისუფლად მოძრაობს ორივე მხარეს, მაგრამ საზოგადოდ ხელმისაწვდომია ინფორმაციული პროცესის ყველა მონაწილისათვის. ეს ეხება მასიური გამოყენებისათვის ღია ინტერნეტის ყველა სამსახურს, მაგრამ ჩვეულებრივი საფოსტო კავშირშიც ღია ბარათების გვერდით არსებობენ საფოსტო კონვერტები. საფოსტო კონვერტების გამოყენება მიმოწერისას არ ნიშნავს რომ პარტნიორებს დასამალი აქვთ რამე. მათი გამოყენება შეესაბამება დიდი ხნით დამკვიდრებულ ისტორიულ ტრადიციებს და საზოგადოების მორალურ-ეთიკურ ნორმებს. ინფორმაციის დასაცავად ანალოგიური „კონვერტების“ საჭიროება ინტერნეტშიც არსებობს. დღეს ინტერნეტი არ წარმოადგენს მარტო ურთიერთობების საშუალებას და უნივერსალურ საცნობარო სისტემას. მასში მოძრაობს სახელშეკრულებო და ფინანსური ვალდებულებები, რომელთა დაცვის აუცილებლობა საჭიროა, როგორც დათვალიერების ისე ფალსიფიკაციისაგან. 1999 წლიდან მოყოლებული ინტერნეტი ხდება ელექტრონული კომერციის მძლავრი საშუალება, ეს კი მოითხოვს საგადასახადო ბარათების და სხვა ელექტრონული გადახდის საშუალებების დაცვას.

ინტერნეტში ინფორმაციის დაცვის პრინციპები ეყრდნობა ინფორმაციის განსაზღვრებას. *ინფორმაცია* არის *მონაცემების* და მათი ადექვატური მეთოდების ურთიერთქმედების პროდუქტი. თუ კომუნიკაციის პროცესში მონაცემები გადაეცემა ღია სისტემით (ხოლო ინტერნეტი ეკუთვნის სწორედ ასეთს), მაშინ მათთან უცხო პირების შეღწევის გამორიცხვა თეორიულადაც კი შეუძლებელია. შესაბამისად, დაცვის სისტემები ორგანიზებულია

ინფორმაციის მეორე კომპონენტზე - მეთოდებზე. მათი მოქმედების პრინციპი დაფუძნებულია იმაზე, რომ გამოირიცხოს ან გართულდეს მაინც მონაცემების ინფორმაციაში გარდაქმნის ადეკვატური მეთოდის შერჩევის შესაძლებლობა. ერთერთ ასეთ მეთოდს წარმოადგენს მონაცემების დაშიფვრა.

4.4 ინფორმაციული უსაფრთხოება

ინფორმაციული უსაფრთხოების აუცილებლობა გამომდინარეობს თვით ქსელის სამსახურების, სერვისების და მომსახურების ბუნებიდან. როგორც უკვე ვთქვით, ნებისმიერი ქსელური სამსახურის საფუძველს შეადგენს პროგრამების წყვილი: სერვერი და კლიენტი, რომლებიც მუშაობენ ერთობლივად დადგენილი წესის მიხედვით. ეს წესები დადგენილია ქსელური სამსახურების პროტოკოლებში. როგორც სერვერის, ისე კლიენტის პროგრამებს, რომლებიც ახორციელებენ ქსელის პროტოკოლებს გააჩნიათ ნებადართული ოპერაციების შესრულების აუცილებელი საშუალებები. ოპერაციები, რომლებიც სცილდებიან პროტოკოლით დადგენილი ოპერაციების ფარგლებს, ითვლებიან არა უსაფრთხოდ. ამასთან ერთად, თუ კი ისინი სრულდებიან უნებართვოდ, მიმდინარე მხარესთან შეუთანხმებლად, ითვლებიან აკრძალულად და ქმნიან ადმინისტრაციული სამართალდარღვევების ან სისხლის სამართლის დანაშაულის შემადგენლობას.

პროტოკოლები - სამუშაო სტანდარტებია. ახალი პროტოკოლები იშვიათად იქმნებიან, ხოლო ძველები მოქმედებენ ძალიან დიდხანს, ათობით წლებით. ამ დროის განმავლობაში ინფორმაციული ტექნოლოგიები უსწრებენ მათ და წარმოიშობა შეუთავსებლობა იმას შორის, რაც ტექნიკურადაა შესაძლებელი

შესრულდეს ქსელში და რაც ნებედართულია მოძველებული პროტოკოლებით. ისწრაფიან რა, გააუმჯობესონ სერვერის და კლიენტის პროგრამებს შორის ურთიერთქმედება, პროგრამისტები განუწყვეტლივ მუშაობენ მათი შესაძლებლობების გაფართოებაზე. აქ წარმოიქმნება წინააღმდეგობა სურვილსა და შესაძლებელს შორის. ასე მაგალითად, იმისათვის, რომ *Web* გვერდები ყოველდღიურად ხდებოდნენ უფრო მიმზიდველნი, პროგრამისტებს შეუძლიათ შემოგეთავაზონ ახალი, საინტერესო მეთოდები და ხერხები, მაგრამ შესძლებს პროგრამა ბრაუზერი შეასრულოს მათი მცდელობები - რთული საკითხია. რჩება რა მხოლოდ პროტოკოლით ნებედართულ მკაცრ ჩარჩოებში, *Web* სერვერი უნაროა ითამაშოს კლიენტთან „კრესტიკი-ნოლიკი“-ც კი. ამიტომ, რომ გააფართოვოს სერვერსა და ბრაუზერს შორის ურთიერთქმედების არეალი, სერვერის მფლობელმა რადაცნაირად უნდა „დაარწმუნოს“ ანდა სხვა წესით „მოურიგდეს“ კლიენტს გააფართოვოს თავისი ბრაუზერის შესაძლებლობები, რასთანაც ხშირად გვაქვს საქმე. სწორედ ამ დროს წარმოიქმნება ქსელის უსაფრთხოების საშიშროება. კლიენტის პროგრამების შესაძლებლობების ნებისმიერი გაფართოება იწვევს სტანდარტული პროტოკოლიდან გარკვეულ გადახვევას, რამაც შეიძლება შექმნას გარკვეული საშიშროება.

ასე მაგალითად, დავაყენეთ რა ბრაუზერის გაფართოებული საშუალებები, რომელიც საშუალებას გვაძლევს ვითამაშოთ „კრესტიკი-ნოლიკი“ სერვერის თხოვნით, საბოლოო ჯამში, შეიძლება მივიღოთ აგენტი, რომელიც სერვერის მართვით დაიწყებს „უფროსობას“ კლიენტის ოპერაციულ სისტემაში. რა თქმა უნდა აქ „კრესტიკი-ნოლიკი“ პირობითი მაგალითია. სინამდვილეში

სერვერები ბრაუზერების მრავალ სხვადასხვა გაფართოებებსა და დამატებებს ვვითავაზობენ, რომლებიც აჩქარებენ *Web*-გვერდების ჩატვირთვას, ქსელში ინფორმაციის ძებნის გამარტივებას, და ა.შ. რა თქმა უნდა შორსა ვართ იმ აზრისაგან რომ, ყველა ახალი ტექნოლოგიები კლიენტის ან სერვერის საზიანოდაა მიმართული. ეს მაგალითი მოგვყავს მხოლოდ იმის გასაგებად, რომ ქსელური უსაფრთხოების საკითხი ფაქიზ ბალანსშია იმას შორის თუ რისი უფლება გვინდა მივცეთ ჩვენს თავს ქსელში და რა დაგვიჯდება ეს უსაფრთხოების თვალსაზრისით. ზოგადი პრინციპი ასეთია: რაც უფრო რთულია სისტემა მით მეტ შესაძლებლობებს იძლევა და მით უფრო რთულია მასში უსაფრთხოების სათანადო დონის კონტროლის უზრუნველყოფა. აქ ყურადღება უნდა გავამახვილოთ სიტყვებზე „უსაფრთხოების სათანადო დონეზე“ ვინაიდან სხვადასხვა კომპიუტერებისათვის იგი სხვადასხვაა. უნდა ავლნიშნოთ, რომ სტანდარტული ქსელური საშუალებები, რომლებიც დგება *Windows*-ის ოპერაციულ სისტემასთან ერთად, არ უზრუნველყოფენ უსაფრთხოების არანაირ დონეს, ამიტომ საუბარი რაიმე სათანადო დონის უსაფრთხოებაზე მასთან მიმართებაში სრულიად უსაფუძვლოა. ამ საშუალებების გამოყენება მოხერხებულია სასწავლო ან საყოფაცხოვრებო დონეზე მაგრამ, როცა საქმე ეხება სამსახურის კომპიუტერების კორპორაციულ დაკავშირებას ინტერნეტთან, აუცილებელია სპეციალური ზომების მიღება: ან უნდა ვუზრუნველყოთ მიერთებული კომპიუტერის „სტერილური სისუფთავე“ ნებისმიერი სახის სამოსამსახურო მონაცემებისაგან, ან გამოვიყენოთ სხვა ოპერაციული სისტემები, ისეთები როგორიცაა *UNIX*, *Linux* და ა.შ.

„სათანადო“ დონის უსაფრთხოების ცნება. უსაფრთხო-

ების დონე, რომელსაც უნდა უზრუნველყოფდეს კონკრეტული კომპიუტერი, დამოკიდებულია კომპიუტერის დანიშნულებაზე. როდესაც საუბარია სასწავლო ან საცნობარო კომპიუტერზე, მაშინ მის უსაფრთხოებაზე ზრუნვა შეიძლება დავიყვანოთ კომპიუტერული ვირუსებისა და სხვა სახიფათო პროგრამებისაგან რეგულარულად დაცვის მომსახურებაზე. კომპიუტერებისათვის, რომლებზეც ინახება კონფიდენციალური მონაცემები, დაცული უნდა იქნას უსაფრთხოების საკმარისი დონე. კონფიდენციალურ მონაცემებს მიეკუთვნება არა მხოლოდ საიდუმლო ცნობები, რომლებსაც აქვთ სახელმწიფო საიდუმლოს ხასიათი, არამედ ჩვეულებრივი პერსონალური მონაცემებიც. მაგალითად, ადამიანების მისამართები, მათი პირადი აღრიცხვის მონაცემები - საპასპორტო, სამედიცინო, განათლების და სხვა, თუ საწარმოში არიან სპეციალისტები, რომლებიც დაკავებული არიან ქსელური უსაფრთხოების საკითხებით, მათ შეუძლიათ უზრუნველყონ კონფიდენციალური მონაცემების უსაფრთხო შენახვა ქსელთან მიერთებულ კომპიუტერზე, მაგრამ ეს მეტად ძვირადღირებული და რთული ღონისძიებაა. თუ საწარმოში ან ორგანიზაციაში ასეთი სპეციალისტები არ არიან, მაშინ არ უნდა მიუერთოთ ის კომპიუტერი ქსელს, რომელზეც კონფიდენციალური მონაცემები ინახება.

მაგალითისათვის განვიხილოთ უნივერსიტეტის ტიპის სასწავლო დაწესებულება. მისი კომპიუტერები განლაგებულია ლაბორატორიებში, ბიბლიოთეკაში და ადმინისტრაციულ განყოფილებებში. თუ ინტერნეტთან კავშირი სასწავლო ლაბორატორიის კომპიუტერებს აქვთ, მაშინ მათზე არ უნდა იყოს არანაირი

კონფიდენციალური მონაცემები: არც მოსწავლეების მისამართები, არც ცნობები მოსწავლეებზე, არც მოსწრების შესახებ ცნობები. მეორეს მხრივ, მსგავსი ცნობები შეიძლება იყოს ადმინისტრაციული განყოფილებების კომპიუტერებზე, მაშასადამე, ამ კომპიუტერების მიერთება ინტერნეტთან სპეციალური დამცავის საშუალებების გარეშე დაუშვებელია. იგივე ეხება ნებისმიერ სახელმწიფო თუ ადმინისტრაციულ დაწესებულებებს, რომლებშიც ინახება სამსახურებრივი მონაცემები ან პერსონალური აღრიცხვის მონაცემები. ქსელთან სამუშაოდ უნდა გამოიყოს კონფიდენციალური მონაცემებისაგან სტერილურად სუფთა განსაკუთრებული კომპიუტერი.

სახელმწიფო საწარმოებში და კომერციულ სტრუქტურებში, უსაფრთხოების რეჟიმის უზრუნველყოფაზე მუშაობენ სპეციალურად მომზადებული ადამიანები - სისტემის ადმინისტრატორები. მათ ამოცანაში შედის ქსელის რეგულარული მონიტორინგი უსაფრთხოების რეჟიმის დარღვევის მეთოდებზე ცნობების შესაგროვებლად, დაცვის გამოცდილი პროგრამული და აპარატურული საშუალებების დაყენება, კონტროლი იმაზე, თუ რა პროგრამებს აყენებენ და როგორ მოიხმარებენ მათ. კომერციული ორგანიზაციების ადმინისტრაცია ინდივიდუალურად უდგება საკითხს იმის შესახებ, თუ მისთვის რაა სასარგებლო: დაიქირაოს მაღალანაზღაურებადი სპეციალისტი მონაცემების დასაცავად და დააყენოს იაფი მოწყობილობა თუ გამოყოს ქსელში სამუშაოდ იაფი კომპიუტერები, რომლებზეც არ ინახება არანაირი კონფიდენციალური მონაცემები და რომლის უსაფრთხოებაც შეიძლება თამამად უგულებელყოფილი იქნას.

რეჟიმულ საწარმოებში ამა თუ იმ კომპიუტერის ქსელთან მიერთების საკითხი თვითოეული სამუშაო ადგილისათვის ინდივიდუალურად წყდება. რა თქმა უნდა, აქ საუბარი არ შეიძლება იყოს ისეთი ტიპის სტანდარტული ქსელური საშუალებების გამოყენებაზე, რომლებიც შედიან Windows სისტემის შემადგენლობაში. მათი ფუნქციონირების უსაფრთხოების მიღწევა ბევრად უფრო ძვირი ღირს (თუ საერთოდ შესაძლებელია) ვიდრე სპეციალური საშუალებების გამოყენება, რომლებმაც ინფორმაციის დაცვის სფეროში გაიარეს სერტიფიცირება სპეციალისტებთან.

4.5 ქსელური უსაფრთხოების რეჟიმის დარღვევის ძირითადი სახეები

დაშორებული ადმინისტრირების საფრთხე დაშორებული ადმინისტრირების ქვეშ იგულისხმება დაშორებული კომპიუტერით არასანქცირებული მართვა. დაშორებული ადმინისტრირება იძლევა სხვისი კომპიუტერის თავისი მართვის ქვეშ მოქცევის საშუალებას. იგი იძლევა მასზე არსებული მონაცემების მოდიფიცირებისა და ასლის გადაღების, ნებისმიერი პროგრამების, მათ შორის საზიანო პროგრამების დაყენების საშუალებას, აგრეთვე ქსელში სხვისი კომპიუტერით „მისი სახელით“ დანაშაულებებრივი ქმედებების ჩადენის შესაძლებლობას.

აქტიური შემადგენლობის საფრთხე აქტიური შემადგენლობა Web-გვერდში ჩართული აქტიური ობიექტია. პასიური შემადგენლობასაგან განსხვავებით (ტექსტები, ნახატები, აუდიოკლიპები და სხვა), აქტიური ობიექტები თავის თავში შეიცავენ არა მარტო მონაცემებს, არამედ პროგრამულ კოდებსაც. აგრესიული პროგრამული კოდი, მოხვედბა რა „მსხვერპლის“ კომპიუტერზე,

შეუძლია მოიქცეს როგორც კომპიუტერული ვირუსი ან როგორც პროგრამა-ავენტი. ასე მაგალითად, მას შეუძლია არ გაანადგუროს მონაცემები, მაგრამ შეუძლია იმოქმედოს დაშორებულ პროგრამებთან ერთად და იმოშაოს როგორც დაშორებული ადმინისტრირების საშუალებამ.

ტრანსპორტირების გზაზე მონაცემების დაჭერისა და შეცვლის საშიშროება. ეკონომიკაში ინტერნეტის გამოყენებისას მწვავედ დგას მონაცემების ტრანსპორტირებისას მათი ხელში ჩაგდებისა და შეცვლის საფრთხე. მაგალითად, ელექტრონული საგადასახადო საშუალებებით ანგარიშსწორება ითვალისწინებს მყიდველის მიერ თავისი ბარათის კონფიდენციალური მონაცემების გადაგზავნას გამყიდველთან. თუ ამ მონაცემებს ხელში ჩაიგდებენ რომელიმე შეაღებულ სერვერებზე, არ არის იმის გარანტია, რომ მას არ გამოიყენებს დამნაშავე.

გარდა ამისა, ინტერნეტით გადაიცემა ფაილები. ამ ფაილების შეცვლამ ტრანსპორტირების გზაზე შეიძლება მიგვიყვანოს იმასთან, რომ ნაცვლად მოთხოვნილი პროგრამისა კლიენტი მიიღებს მის ანალოგს „გაფართოებული“ თვისებებით.

პირად ცხოვრებაში ჩარევის საფრთხე. ამ საფრთხეს საფუძვლად უდევს სარეკლამო ორგანიზაციების კომერციული ინტერესები. ამჟამად, ინტერნეტის წლიური სარეკლამო ბიუჯეტი შეადგენს რამოდენიმე ათეულ მილიარდ ამერიკულ დოლარს. რეკლამიდან შემოსავლის გაზრდის სურვილით მრავალი კომპანიები ქმნიან Web-კვანძებს არა იმდენად იმისათვის, რომ კლიენტებს მიაწოდონ ქსელის სამსახურები, არამედ იმისათვის, რომ შეაგროვონ პერსონალური მონაცემები მათზე. ეს მონაცემები განზოგადდებიან, კლასიფიცირდებიან და მიეწოდებათ სარეკლამო

და მარკეტინგულ სამსახურებს. პერსონალური ინფორმაციის შეგროვების პროცესი ავტომატიზირებულია, პრაქტიკულად არ მოითხოვს არავითარ დანახარჯებს და საშუალებას იძლევა კლიენტის დაუკითხავად გამოიძიოს მისი გემოვნება, მიდრეკილებები, ინტერესის სფეროები და სხვა..

მიუღებელი შემადგენლობის დოკუმენტის მიღების საფრთხე ინტერნეტში გამოქვეყნებული ყველა ინფორმაცია არ შეიძლება ჩაითვალოს საზოგადოებრივად სასარგებლოდ. არსებობს მორალურ-ეთიკური, რელიგიური, კულტურული და პოლიტიკური ხასიათის მრავალი მიზეზები, როდესაც საზოგადოებისათვის უსიამოვნოა მოწოდებული ინფორმაცია და სურს მისგან თავის დაცვა.

მსოფლიოს მრავალ ქვეყანაში ინტერნეტი ჯერ კიდევ არ ითვლება მასიური ინფორმაციის საშუალებად. ეს დაკავშირებულია იმასთან, რომ მოწოდებული არ ახდენს მის გამრავლებას და გავრცელებას, ანუ ის არ ასრულებს მასიური ინფორმაციის საშუალებების ფუნქციებს. ყოველივე ამას კლიენტი თვითონ აკეთებს ჰიპერმიმართვების გამოყენების მომენტში. ამიტომ ჩვეულებრივ, კანონები მასიური ინფორმაციის საშუალებებზე, რომლებიც არეგულირებენ თუ რა შეიძლება გავრცელდეს და რა არა, ინტერნეტში ჯერ არ მუშაობს.

როგორც ჩანს ამ საკითხში სამართლებრივი ვაკუუმი თანდათანობით ამოიფხვრება, მაგრამ, მრავალ ადამიანს დღეს ჭირდება მიუღებელი შინაარსის დოკუმენტების მოწოდებისაგან დაცვის საშუალებები. ჩვეულებრივად მოწოდებული შემადგენლობის ფილტრაციის ფუნქციებს ავალდებენ ბრაუზერებს, ან ამ მიზნით სპეციალურად დაყენებულ პროგრამებს.

დაშორებული ადმინისტრირებისაგან დაცვა დაშორებული ადმინისტრირებისაგან ეფექტურად თავის დასაცავად აუცილებელია წარმოვიდგინოთ ის მეთოდები, რომლითაც ისინი მიიღწევა. ასეთი მეთოდი ორია. პირველი მეთოდი ემყარება „მსხვერპლის“ კომპიუტერებზე იმ პროგრამის დაყენებას (სერვერის ანალიზი), რომლითაც შეუძლია დამნაშავეს შექმნას დაშორებული შეერთება იმ დროს, როდესაც „მსხვერპლი“ ინტერნეტში იმყოფება. ამ მიზნით გამოყენებულ პროგრამებს „ტროიანულს“ უწოდებენ. თავიანთი ნიშნების მიხედვით ისინი მნიშვნელოვანწილად მოგვაგონებენ კომპიუტერულ ვირუსებს.

დაშორებული ადმინისტრირების მეორე მეთოდი ემყარება იმ ნაკლის გამოყენებას, რომელიც აქვს კავშირში მყოფი პარტნიორების კომპიუტერული სისტემის პროგრამულ უზრუნველყოფას. ამ მეთოდის მიზანია კლიენტის პროგრამასთან ურთიერთობის ფარგლებიდან გასვლა და ოპერაციულ სისტემაზე პირდაპირი ზემოქმედება, რომ მისი საშუალებით მიიღოს სხვა პროგრამებთან და მონაცემებთან შეღწევის საშუალება. პროგრამებს, რომლებიც იყენებენ კომპიუტერული სისტემის შეცდომებს ექსპლოიტებს უწოდებენ.

ტროიანული პროგრამებისაგან დაცვა ტროიანული პროგრამებით კომპიუტერის დასაზიანებლად საჭიროა ვიდაცამ ან რაღაცამ გაუშვას ეს პროგრამა ამ კომპიუტერზე.

- ✓ საჭიროა შეიზღუდოს უცხო პირის დაშვება ქსელურ კომპიუტერთან. შეღწევა იზღუდება ჩვეულებრივი ადმინისტრაციული მეთოდებით (შეღწევის ფიზიკური შეზღუდვა, პაროლით დაცვა და სხვა).

- ✓ უცხო კომპიუტერებზე ტროიანული პროგრამების დაყენების ჩვეულებრივი მეთოდია მომხმარებელზე ფსიქოლოგიური ზემოქმედება. პრინციპი მარტივია. თუ რაიმე არ შეიძლება გააკეთოთ ჩვენ თვითონ, ე.ი. უნდა დავარწმუნოთ მომხმარებელი ეს თვითონ გააკეთოს. ძალიან ხშირად გამოიყენება ზიანის მატარებელი პროგრამების დაზავება ელექტრონული ფოსტის შეტყობინებასთან ერთად დანართის სახით. შეტყობინების ტექსტში მითითებულია თუ რამდენად სასარგებლოა და ხელსაყრელია ეს პროგრამა.
- ✓ არასდროს არ გაუშვიათ ის, რაც მოდის ელექტრონულ ფოსტასთან ერთად, მიუხედავად იმისა თუ რაა დაწერილი თანდართულ შეტყობინებაში. ეს წესი ვრცელდება ახლობლების, მეგობრების, ნაცნობებისაგან მიღებულ ბარათებზეც. ბოროტმზრახველებს აქვთ გამგზავნის მისამართის მიმსგავსების საშუალება ისე, რომ მათი ბარათი გამოიყურებოდეს, როგორც ნაცნობის ბარათი. არის შემთხვევები როდესაც ტროიანული პროგრამები ვრცელდება ცირკულარული ბარათების - „გამოიყენე და გადაეცი მეგობარს“ - სახით, ეს კიდევ საფრთხის ერთი წყაროა, რომელიც იმალება ახლო მეგობრებისაგან მიღებულ ბარათებში.
- ✓ არასდროს არ გაავზავნოთ პროგრამები ელექტრონული ფოსტის დანართების სახით. თუ საჭიროა კოლეგას გადასცეთ სასარგებლო პროგრამა, უმჯობესია მიუთითოთ URL-მისამართი, რომელთაც თვითონ შეძლებს მიიღოს იგი. თვითოეულ, ნამდვილად სასარგებლო პროგრამას ინტერნეტში აქვს თავისი წყარო. თუ პროგრამა ქსელში არაა წარმოდგენილი, ე.ი. არავინ არ იღებს პასუხისმგებლობას მის მუშაობაზე.

- ✓ ელექტრონული ფოსტის გარდა ბოროტმზრახველები ტროიანულ პროგრამებს კომპაქტ-დისკებითაც ავრცელებენ. პრინციპულად არ არის არავითარი აუცილებლობა შევიძინოთ ინტერნეტის პროგრამები კომპაქტ-დისკებზე კრებულის სახით. თვითონ ინტერნეტში არის მრავალი ათასი სასარგებლო პროგრამა, რომლებიც ვრცელდება უფასოდ ან პირობითად უფასოდ.
- ✓ არასდროს არ დააყენოთ ქსელის სამსახურებრივ კომპიუტერებზე შეუმოწმებელი პროგრამული უზრუნველყოფა, რომელიც გავრცელებულია კომპაქტ-დისკებზე კრებულის სახით.

პროგრამული უზრუნველყოფის ექსპლოატაციის შეცდომებისაგან დაცვა. საფრთხის ეს სახე იშვიათადაა საშიში კლიენტისათვის. პროგრამა-ექსპლოიტების შეტევა საფრთხეს ძირითადად სერვერებს უქმნის. ბოროტმზრახველების სტრატეგია ჩვეულებრივად სამ ეტაპედ ხორციელდება, პირველ ეტაპზე ისინი არკვევენ პროგრამებისა და მოწყობილობების შემადგენლობას „მსხვერპლის“ ლოკალურ ქსელში. მეორე ეტაპზე იკვლევენ მოცემულ პროგრამებში ცნობილ შეცდომებს. მესამე ეტაპზე ამზადებენ პროგრამა-ექსპლოიტებს (ან იყენებენ ვიდაცის მიერ მომზადებულ პროგრამებს) აღმოჩენილი შეცდომების ექსპლოატაციისათვის. ბოროტ მზრახველებთან ბრძოლა შეიძლება მოხდეს ყველა სამ ეტაპზე.

უპირველესად, სერვერების ადმინისტრაცია აკონტროლებს გარე მიმართევებს, რომელთა მიზანია სერვერის აპარატულ-პროგრამული კონფიგურაციის გაგება. ეს საშუალებას იძლევა დამრღვევის აღრიცხვაზე ასაყვანად მანამდე, სანამ იგი განახორციელებს რეალურ შეტევას. უფრო საპასუხისმგებლო

შემთხვევებში იყენებენ გამოყოფილ კომპიუტერს ან პროგრამას, რომელიც ასრულებს ქსელთაშორის ეკრანის (ფარის) ფუნქციას. ასეთ საშუალებებს ბრანდმაუერებს (*Firewall*) უწოდებენ. დასაცავად ბრანდმაიერებს შუალედური მდგომარეობა უკავიათ კომპიუტერებსა და გარე სამყაროს შორის. იგი არ იძლევა გარედან სერვერის პროგრამული უზრუნველყოფის დათვალიერების საშუალებას და არ ატარებს არასანქცირებულ მონაცემებსა და ბრძანებებს.

გარდა ამისა, სერვერის ადმინისტრაციამ ყურადღებით უნდა აღეწოს თვალი ისეთი შეტყობინებების პუბლიკაციებს ქსელში, რომლებიც ეხება მის მიერ გამოყენებულ პროგრამებში აღმოჩენილ შეცდომებს. შეცდომები დაუყონებლივ უნდა გამოასწორონ მათზე გამოქვეყნებული ცნობების მიღებისთანავე. ყველაზე მეტად საშიშია შეცდომების აღმოჩენის და მისი გამოსწორების შუა პერიოდი. მიიღებენ რა შეტყობინებას არსებული შეცდომების შესახებ, ბოროტმზრახველები იწყებენ იმ სერვერების მიზანმიმართულ ძებნას, რომელზეც შეცდომები არ არიან გამოსწორებული.

აქტიური შემადგენლობის საფრთხე. როგორც უკვე ავღნიშნეთ, Web-გვერდების შემადგენლობაში შეიძლება შედიოდნენ ჩართული ობიექტები. ისეთი ელემენტები, როგორიცაა სურათები, ვიდეოკლიპები და ხმოვანი ობიექტები წარმოადგენენ პასიურ ელემენტებს. ეს მონაცემები შეიძლება დაავთვალიეროთ, გავახმოვანოთ, შევასწოროთ, შევინახოთ და სხვა. მასზე შეიძლება შევასრულოთ ყველა ის ოპერაციები რაც საკუთარი კომპიუტერების მონაცემებზე. მაგრამ, ბრაუზერის და სერვერის შესაძლებლობების გაფართოების მიზნით, Web-გვერდების

შექმნელების უმეტესობა მათში აქტიურ ელემენტებსა და სცენარებს რთავენ. როგორც ერთ ისე მეორე შემთხვევაში საუბარია კლიენტის მიერ მიღებულ *Web* გვერდის შემადგენლობაში პროგრამული კოდის არსებობაზე.

აქტიური ობიექტები პასიურისაგან განსხვავდებიან იმით, რომ მონაცემების გარდა შეიცავენ კიდევ პროგრამულ კოდს, რომელიც მუშაობს კლიენტის კომპიუტერზე. ყველაზე ზოგად შემთხვევაში სერვერს შეუძლია მოგვაწოდოს ნებისმიერი ბუნების აქტიური ელემენტები. ამისათვის მან მხოლოდ უნდა „დაარწმუნოს“ მომხმარებელი, რომ მან მიიღოს რომელიღაც პროგრამული კოდი, რომელიც აფართოებს მისი ბრაუზერის შესაძლებლობებს. ჩვენ ვვულისხმობთ, რომ მომხმარებელი არანაირ მომხიბვლელ წინადადებაზე არ დათანხმდება, და მაშინ მისთვის საშიშ ობიექტად და სცენარებად რჩებიან მხოლოდ *JavaScript* და *VBScript*. მასთან სამუშაოდ ბრაუზერი უკვე მომართულია.

აქტიური შემადგენლობადან დაცვა. მხარემ, რომელიც თავს იცავს აქტიური ელემენტებისაგან, უნდა შეაფასოს თავისი კომპიუტერის საფრთხე და შესაბამისად გამართოს ბრაუზერი ისე, რომ საფრთხე იყოს მინიმალური. თუ არავითარი მნიშვნელოვანი მონაცემები და კომფიდენციალური ცნობები არ ინახება კომპიუტერზე შეიძლება ამორთოთ დაცვა და დაათვალიეროთ *Web*-გვერდი იმ სახით, როგორც მოგაწოდათ შექმნელმა. თუ საფრთხე არასასურველია, მაშინ ჯავა აპლეტები, *Active X* ელემენტები და აქტიური სცენარები შეიძლება ამორთოთ. კომპრომისული ვარიანტია ყოველ კონკრეტულ შემთხვევაში მოვითხოვოთ ამა თუ იმ აქტიური ობიექტის მიღებაზე ნებართვა. იმის მიხედვით თუ

რომელ კვანძთანაა დამყარებული კავშირი (სანდოა იგი თუ არა) ეს საკითხი ყოველჯერზე სხვადასხვანაირად წყდება.

პროგრამაში *Internet Explorer* აქტიური ელემენტებისაგან დაცვის საშუალებების გამართვა სრულდება დიალოგურ ფანჯარაში „უსაფრთხოების წესები“, (▶ Internet Property ▶ Security ▶).

ტრანსპორტირების გზებზე მონაცემების დაცვის საშუალებები. კომერციის შეტანით ინტერნეტში სულ უფრო ხშირად წარმოიქმნება დისტანციური საქმიანი მოლაპარაკებების საჭიროება, ქსელში პროგრამული უზრუნველყოფის შექმნა, მოწოდებული საქონლისა და მომსახურების ფულადი ანგარიშგების წარმოება. ასეთ შემთხვევაში ტრანსპორტირების გზაზე მონაცემების დაცვის მოთხოვნილებასთან ერთდროულად წარმოიქმნება პარტნიორების დადასტურების (იდენტიფიკაციის) და მონაცემების მთლიანობის დადასტურების (აუტენტიფიკაციის) მოთხოვნილება.

მოვიყვანოთ მაგალითს თუ რაში შეიძლება გამოიხატოს დაცვის უქონლობა და მონაცემების მთლიანობის დადასტურების აუცილებლობა.

1. ერთმანეთისაგან დაშორებული ორი მეწარმე, რომლებიც ერთმანეთს არასდროს არ შეხვედრიან პირადად სდებენ ხელშეკრულებას ერთობლივ საქმიანობაზე. თუ არ იქნება მიღებული სპეციალური ზომები რამოდენიმე ხნის შემდეგ ნებისმიერმა ერთერთმა მხარემ შეიძლება განაცხადოს, რომ მან ხელშეკრულების შესახებ არაფერი იცის და თუ ვისთან ჰქონდა მოლაპარაკება მეორე პარტნიორს მისთვის უცნობია.
2. საქონლისა და მომსახურების შექმნის ანგარიშსწორება ინტერნეტით ჩვეულებრივად საგადასახადო ბარათით

ხდება. მიუხედავად ამისა, მნიშვნელოვან როლს ასრულებს კონფედერაციულ მონაცემებს თავის საკრედიტო ბარათზე და მას შეუძლია ჩამოწეროს ანგარიშიდან შეთანხმებული თანხა. იმ შემთხვევაში თუ ეს მონაცემები „გამოჭერილი“ იქნება ერთ-ერთ რომელიმე შუალედურ სერვერზე, უცნობ პირებს შეუძლია ისარგებლონ სხვისი საკრედიტო ბარათით, გადაიხადოს ამ ბარათით ინტერნეტში შეკვეთები საქონელზე ან მომსახურებაზე.

3. მივიღეთ, რა დაშორებული სერვერიდან სასარგებლო პროგრამა და დავაყენეთ ჩვენ კომპიუტერზე, შეგვიძლია აღმოვაჩინოთ რომ იგი შეიცავს ტროიანულ კოდს, რომელიც შესაძლებლობას აძლევს მათ „იუფროსონ“ ჩვენს კომპიუტერზე. პროგრამის ავტორთან, რომელმაც მოგვაწოდა იგი პრეტენზიებით მიმართვისას შეიძლება მოვისმინოთ პასუხი, რომ არაფერი ამის მსგავსი მას არ გაუვრცელებია, ხოლო თუ სადღაც ტრანსპორტირების გზაზე, ვიღაცამ შეიტანა პროგრამაში არასანქცირებული ცვლილებები, ის ამაზე პასუხს არ აგებს.

ეს მხოლოდ სამი მაგალითია: სინამდვილეში, ეკონომიკაში და ბიზნესში ელექტრონული კომერციის გაჩენიდან ყოველდღიურად წარმოიქმნება უამრავი პრობლემები. დღითი დღე მათი მათი რიცხვი პროგრესულად გაიზრდება. ელექტრონულ კომერციაში დღეს იცავენ და აუტენტიფიცირებას უკეთებენ მონაცემებს, აგრეთვე იდენტიფიცირებას უკეთებენ დაშორებულ პარტნიორებს კრიპტოგრაფული მეთოდებით (თუ როგორ ხორციელდება ეს ოპერაციები, „ელექტრონული ხერმოსწერის რეჟიმის ტექნიკური და იურიდიული უზრუნველყოფა“ და „ელექტრონული

კომერციის ინფორმაციული ტექნოლოგიები“ არ განიხილება ამ წიგნის ფარგლებში) .

პირად ცხოვრებაში ჩარევისაგან დაცვა, დაშორებულ კომპიუტერებზე, გარდა აქტიური ზემოქმედების საშუალებისა არსებობს ინტერნეტის მონაწილეების საქმიანობაზე პასიური დაკვირვების საშუალებები. ისინი გამოიყენებიან სარეკლამო-მარკეტინგული სამსახურის მიერ.

ნებისმიერი Web-გვერდის ნახვისას თვალში გვეცემა სარეკლამო განცხადებები (მათ ბანერებს უწოდებენ). მათი მიღებისას ბრაუზერი ამყარებს კავშირს მათ მფლობელებთან (სარეკლამო სისტემასთან) და ჩვენს შეუმჩნეველად რეგისტრირდება ამ სისტემაში. ჩვენ შეიძლება არ მივაქციოთ ყურადღება ამ რეკლამას და იგი არსდროს გამოვიყენოთ, მაგრამ გადავდივართ რა ერთი Web გვერდიდან მეორეზე ვქმნით ჩვენს ფსიქოლოგიურ პორტრეტს (მას „პროფილი“ ეწოდება). მონახულებული Web-გვერდებისა და Web-კვანძების ხასიათის მიხედვით დაშორებულ სამსახურს შეუძლია განსაზღვროს სქესი, ასაკი, განათლების დონე, საქმიანობის სახე, ინტერესების სფერო, კეთილდღეობის დონე და აგრეთვე დაავადების ხასიათი და სახეც, რომელიც მას არასოდეს უნახავს. საკმარისია, თუნდაც ერთხელ დარეგისტრირდეთ სადღაც თქვენი სახელით და გვართ, და ადრე შეგროვებული აბსტრაქტული ცნობები იძლევიან სრულიად კონკრეტულ ხასიათს - ამდაგვარად ინტერნეტის მონაწილეებზე იქმნება ფარული პერსონალური მონაცემთა ბაზები.

სხვადასხვა ადამიანებზე ან ერთი და იგივე ადამიანზე სხვადასხვა დროს მიღებული მონაცემების შედარებით მოთვალთვალე სისტემები იღებენ პროფილს არა მარტო ცალკეულ

ადამიანზე არამედ ჯგუფებზე: ოჯახები, მუშა ჯგუფები, საწარმოები. მიღებული მონაცემები შეიძლება გამოიყენონ, როგორც ლეგალურად ასევე არალეგალურად. მაგალითად, აიგივებს რა რომელიმე პირს, როგორც სამთო თხილამურების მოყვარულს, სარეკლამო სისტემა მას მომდევნო გასვლისას ინტერნეტში ხშირად წარუდგენს განცხადებას, რომელიც მიეკუთვნება ამ სახის სპორტს და არა სხვას. ეს ცნობების ლეგალური გამოყენების მაგალითია. მაგრამ არის არალეგალური გამოყენების მაგალითებიც. კლასიფიცირებული მონაცემთა ბაზები საქონელს წარმოადგენს: მათ ყიდულობენ და ყიდიან, გადადიან ხელიდან ხელში და ხდება სრულიად სხვადასხვა პროფილის ორგანიზაციების საქმიანობის საფუძველი.

პერსონალური ინფორმაციის წყაროები. უფრო მარტივ და თვალსაჩინო წყაროს ინტერნეტის აქტიურ კლიენტებზე ცნობების შესაგროვებლად წარმოადგენს მარკერი-*Cookie*; რომლის მოქმედების პრინციპსაც აქ განვიხილავთ.

HTTP (Hyper Text Transler Protocol) პროტოკოლის თანახმად ბრაუზერს შეუძლია გაუგზავნოს სერვერს მოთხოვნა ერთი *Web*-რესურსის მოწოდებაზე (*HTML* დოკუმენტის) და ამასთან არა-ნაირად არ წარუდგინოს თავი სერვერს. ე.ი. თავის საფუძველში, *WWW* სამსახური ანონიმურია. (ყოველ შემთხვევაში ასეთი უნდა იყოს). მიუხედავად ამისა, ხანდახან მიზანშეწონილია ბრაუზერი „წარუდგეს“ სერვერს. ეს მაგალითად სასარგებლოა ინტერნეტ მაღაზიებისათვის. თუ წიგნების ელექტრონულ მაღაზიაში ეკონომიკას მიძღვნილი რამოდენიმე წიგნი მომხმერებლის „კალათში“ გადავდეთ, ხოლო შემდეგ გადავედით სხვა *Web*-გვერდზე, რომელიც იურისპრუდენციას ეძღვნება, არ იქნებოდა სასურველი, რომ

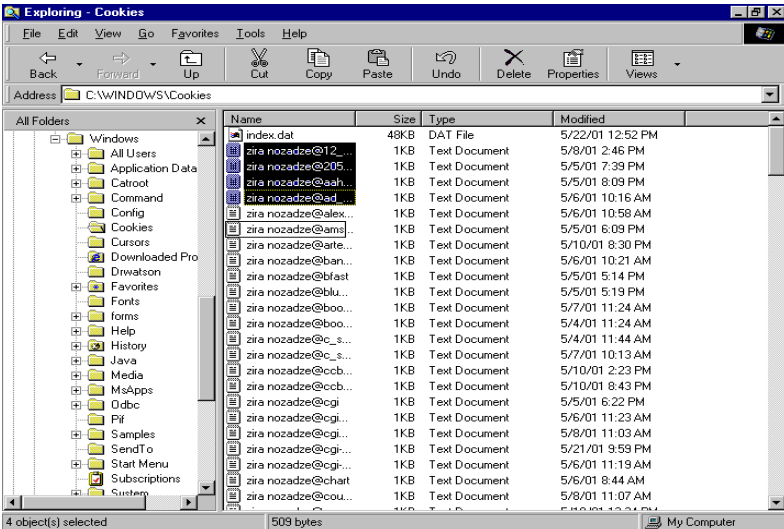
ჩვენი „კალათა“ დაიკარგოს. ანუ ახალ გვერდზე შესვლისას სასურველია რომ სერვერმა დაგვიმასხვროს და გააგრძელოს დაწყებული სამუშაო.

ბრაუზერის სერვერზე წარდგინების მიზანშეწონილობა წარმოიქმნება ყოველთვის, როდესაც კლიენტი სარგებლობს *Web*-სამსახურით, რომელიც პერსონალურად მასზეა მომართული. განჭვრიტეს რა ეს მიზანშეწონილობა, თითქმის ათი წლის უკან, *HTTP* პროტოკოლის დამმუშავებლებმა გაითვალისწინეს მარტივი და როგორც მაშინ მათ ეჩვენებოდათ, სრულიად უწყინარი მექანიზმი ბრაუზერის სერვერისათვის წარსადგენად ე.წ. მარკერების *cookie* საშუალებით.

HTTP-პროტოკოლის თანახმად, სერვერს შეუძლია გადასცეს ბრაუზერს მონაცემების მცირე პაკეტი, რომელშიც დაშიფრულია სერვერისათვის ბრაუზერის იდენტიფიკაციისა და მასთან სამუშაოდ მომართვისათვის საჭირო ინფორმაცია. ეს პაკეტი დროებით იმასხვრება კომპიუტერის ოპერაციულ მეხსიერებაში და ასრულებს სერვერის ფუნქციას. თუ *WWW*-ში მუშაობისას ბრაუზერი კვლავ მიმართავს იგივე *Web*-კვანძს, მაშინ მიმართვისას იგი წარუდგენს ადრე მიღებულ მარკერს, და სერვერი მაშინვე აღითქვამს რომელ კლიენტთან აქვს საქმე.

მარკერები შეიძლება იყოს დროებითი ან მუდმივი. დროებითი მარკერი ინახება ოპერაციულ მეხსიერებაში სანამ ბრაუზერი მუშაობს. მისი მუშაობის დამთავრების შემდეგ სერვერისაგან მიღებული ყველა დროებითი მარკერი ნადგურდება. პრინციპში, უმრავლეს შემთხვევაში, ისეთებში როგორცაა ინტერნეტ-მაღაზიების „სტუმრობა“, შეიძლება შემოვიფარგლოთ დროებითი მარკერებით, რათა მაღაზიამ „არ დაივიწყოს“ თავისი კლიენტი,

როდესაც ის გადაინაცვლებს ერთი განყოფილებიდან მეორეში. მაგრამ სერვერები, გაუგებარი მიზეზების გამო ამჟღახობენ ბრაუზერს გაუგზავნონ არა დროებითი არამედ მუდმივი მარკერები. მუდმივი მარკერები სხვანაირად მუშავდებიან. როდესაც ბრაუზერი ამთავრებს მუშაობას, ოპერატიულ მეხსიერებაში დაგროვილი ყველა მუდმივი მარკერი გადაიტანება ხისტ დისკზე *Cookie*-ფაილების სახით. ასე ხდება ხისტი დისკის მარკირება და შეიძლება ითქვას არა მარტო ხისტი დისკის, არამედ საერთოდ კლიენტის კომპიუტერის. მომდევნო გასვლისას ინტერნეტში, ბრაუზერის გაშვების მომენტში, ხდება დაგროვილი *Cookie*-მარკერების წაკითხვა ოპერატიულ მეხსიერებაში, საიდანაც ბრაუზერი წარუდგენს მათ იმ სერვერებს, რომლებმაც ისინი მოგვაწოდეს.



სურ 4. *Cookie*-მარკერების დათვალიერება.

Cookie მარკერები კომპიუტერებისათვის ფიზიკურ საფრთხეს არ უქმნიან. ეს მონაცემების ფაილია, რომლებიც არ

წარმოადგენენ პროგრამულ კოდს და ამიტომ უსაფრთხოა არასანქცირებული მოქმედების თვალსაზრისით. მაგრამ ისინი წარმოადგენენ საფრთხეს პირად ცხოვრებაში ჩარევის თვალსაზრისით.

WWW-ში ნავიგაციის დროს შეკრებილი *Cookie* მარკერები ინახებიან პაპკაში *C:\Windows\Cookie*. სურათზე 4, გამოყოფილია იმ Web-კვანძების მარკერები, რომლებსაც საერთოდ არ წვევიან. ეს Web-კვანძები *Cookie* მარკერებს იყენებენ WWW-ს კლიენტებზე ფარული დაკვირვებისათვის.

Cookie-მერკერების სამართლებრივი რეჟიმი. კლიენტზე მონაცემების არასანქცირებული შეკრებისათვის *Cookie*-მერკერების გამოყენების სულ მცირე, ორი მექანიზმი არსებობს. უფრო თვალსაჩინოა არალეგალური მექანიზმი, დაკავშირებული იმასთან, რომ სერვერებს შეუძლიათ წაიკითხონ არა მარტო ის მარკერები, რომლებიც თვითონ მოგვაწოდა არამედ სხვა სერვერების მარკერებიც. ეს მეთოდი ბრაუზერით უნდა დაიბლოკოს, მაგრამ ისტორიამ იცის მრავალი შემთხვევა, როდესაც პროგრამისტების შეცდომის გამო, სერვერებს მაინც ჰქონდათ საშუალება მიეღოთ ეს მონაცემები. არ არის გამორიცხული, რომ ასეთი შეცდომები ამჟამადაც არის ხმარებულ ბრაუზერებში ან თვით ოპერაციულ სისტემაში. ამ მეთოდს ვუწოდებთ არალეგალური, რადგანაც შეცდომების და კომპიუტერული სისტემის „მტკივნეული“ ადგილების გამოყენება სამართალდარღვევაა.

კლიენტებზე ცნობების შეგროვების მეორე მექანიზმი *Cookie*-მერკერების საფუძველზე სრულიად ლეგალურია და ბოლო დროს ფართოდ შევიდა პრაქტიკაში. ის დამყარებულია იმაზე, რომ რომელიმე სამსახური (მაგალითად სარეკლამო) ფართოდ

ავრცელებს სხვადასხვა თემატიკური მიმართულების *Web* კვანძების დიდ რაოდენობაზე თავის გრაფიკულ ობიექტებს, მაგალითად სარეკლამო ბანერებს. *Web*-კვანძის დამოვალიერებლები სარეკლამო ბანერებთან ერთად იღებენ მათთან მიბმულ *Cookie*-მერკერებს. საბოლოოდ მიიღება, რომ სამსახურები, რომლებისთვისაც კლიენტს არასოდეს არ მიუმართავს მონიშნავენ მათ კომპიუტერს თავისი მერკერებით, რომლის მიხედვითაც, შემდგომში ზუსტად შეიძლება აღადგინოს ინტერნეტის *Web*-გვერდებზე კლიენტის მოძრაობის სურათი. ამას აკეთებენ არა მარტო სარეკლამო კომპანიები, არამედ კომპანიებიც, რომლებიც გვთავაზობენ სხვა სამსახურებსაც, მაგალითად თავისი დამკვეთების *Web*-გვერდების მნახველების მოვლელების დაყენება.

Cookie-მერკერების გამოყენების პრაქტიკა ინტერნეტის მომხმარებლებზე ცნობების შესაკრებად, ამჟამად სამართალმცოდნე სპეციალისტების დაჟინებული ყურადღების ქვეშაა. მასში ეჭვს იწვევს მონაცემების შეკრების დაფარვის ფაქტი. მომხმარებლის წინააღმდეგობას ამ ფაქტზე ძირითად წარმოადგენს ბრაუზერის იმ ფუნქციების ამორთვის საშუალება, რომლებიც დაკავშირებულია მარკერების მოწოდებასთან. მაგრამ, აქაც არის იურიდიული შეუსაბამობა. საქმე იმაშია, რომ ინტერნეტით სარგებლობენ არასრულწლოვანი პირები. არასრულწლოვანი პირებისაგან მიღებული ცნობების სამართლებრივი რეჟიმი საეჭვოა. ამჟამად, მთელ რიგ ქვეყნებში მუშავდება შეზღუდვები მარკერების გამოყენებაზე იმასთან დაკავშირებით, რომ სერვერს უნდა ჰქონდეს კლიენტის სამართლებრივი სტატუსის იდენტიფიკაციის ობიექტური საშუალებები, სანამ მის კომპიუტერზე განათავსებს მარკერებს. იგულისხმება, რომ მან უნდა გასცეს აუცილებელი

გაფრთხილებები და იმ შემთხვევაში თუ მისი მომსახურებით სარგებლობენ არასრულწლოვანი პირები, თავი შეიკავონ მარკერების, როგორც დაყენებისაგან ასევე ადრე დაყენებული მარკერების წაკითხვისაგან. ასეთი მიდგომა უთუოდ ხელს შეუწყობდა კლიენტების შესახებ ინფორმაციის ფარული შეგროვების შეწყვეტას.

პერსონალური ინფორმაციის სხვა წყაროები. Cookie-მერკერების გარდა ქსელის კლიენტებზე ცნობების შეგროვების წყაროს წარმოადგენს ბრაუზერის მიერ ლეგალურად მოწოდებული ინფორმაცია. *HTTP* პროტოკოლით კავშირის დროს ბრაუზერი ატყობინებს თავის დასახელებას, ვერსიის ნომერს, კომპიუტერი-კლიენტის ოპერაციული სისტემის ტიპს და იმ *Web*-გვერდის *URL*-მისამართს, რომელსაც კლიენტმა მიმართა ბოლოს.

ამას გარდა, სერვერებს გააჩნიათ მეთოდები, რომლებიც საშუალებას იძლევიან ზოგიერთ შემთხვევაში მიიღოს კლიენტის ელექტრონული ფოსტის მისამართი, თუმცა ეს მეთოდები არალეგალურად გამოიყენებიან და ამიტომ მათი სამართლებრივი რეჟიმი საეჭვოა.

პერსონალური ინფორმაციის კიდევ ერთ წყაროს წარმოადგენს ვერტე წოდებული აქტიური სცენარები - *Java Script* (*Java* სკრიპტები). მათთან დაკავშირებული დაცვის სისტემის ნაკლის განხილვა სცილდება ამ წიგნის ფარგლებს).

4.6 ინტერნეტის ზოგიერთი სასარგებლო გვერდები

ინტერნეტში მიმართვების კომპაქტური ნაკრების მოცემა თითქმის შეუძლებელია. ერთი მხრივ შეუძლებელია ყველასათვის საინტერესო მიმართვების შერჩევა, მეორეს მხრივ ინტერნეტში გვერდები განუწყვეტლივ ჩნდება და ქრება. ასე რომ, ნებისმიერი ცნობარი მაშინვე მოქველებული ხდება.

ინფორმაციული სერვერის ამა თუ იმ კატეგორიასთან მიკუთვნება უკიდურესად პირობითია. როგორც წესი, გარდა ძირითადი თემატიკისა სერვერზე გამოიტანება ინფორმაცია, რომელიც მის შემქმნელს საინტერესო ეჩვენება. ამიტომ აქ არ შევეცდებით ინტერნეტის გვერდების რაოდენობით გატაცებას, არამედ მკითხველს მივცემთ საშუალებას თითონ გაერკვეს ინფორმაციის ამ ოკეანეში.

ინტერნეტის საძიებო სერვერები

- **<http://www.yahoo.com/>**

ყველაზე პოპულარული საძიებო სერვერია. სტატისტიკის მიხედვით მთელი ინფორმაციის ძებნის მოთხოვნების ორი მესამედი სწორედ ამ სერვერზე მოდის. ამას გარდა, სერვერზე წარმოდგენილია ინფორმაციული რესურსების კლასიფიკაცია (Yellow Pages).

- **<http://www.altavista.com/>**
- **<http://www.excite.com/>**
- **<http://www.hotbot.com/>**
- **<http://www.infoseek.com/>**
- **<http://www.excite.com/>**
- **<http://www.lycos.com/>**

- <http://www.opentext.com/>
- <http://www.webcraivier.com/>
- <http://www.excite.com/>
- <http://www.askjeeves.com/>
- <http://www.dejanews.com/>

ეს სერვერი შეიცავს ტელეკომფერენციების მილიონობით წერილს. ძებნა ხორციელდება ამ მასალების მიხედვით.

FTP ძებნა

- <http://www.download.com/>

Download.com წარმაადგენს CNET (The Computer Network) ქსელის სერვერს. იგი შეიცავს კატეგორიების მიხედვით კლასიფიცირებულ პროგრამებს: კომერციული პროგრამების დემო-ვერსიებს, დრაივერებს, კომერციულ პროდუქტებში დაშვებული შეცდომების გამსწორებელ პროგრამებს.

- <http://www.filez.com/>

ამ კვანძის საშუალებით ხორციელდება ინტერნეტში ფაილების ძებნა.

- <http://www.filez.com/>

შეიცავს 200 ათასზე მეტ თავისუფლად გასავრცელებელ პროგრამებს. პოროგრამული ყზრუნველყოფა კლასიფიცირებულია კატეგორიებად: ბიზნესი, თამაშები, სასკოლო პროგრამები და ა.შ.

ელექტრული ფოსტის მისამართების ძებნა

როგორც WWW – სერვერების საძიებო სისტემების შემთხვევაში, საძიებო ტექნოლოგიები დაფუძნებულია იმ ინფორმაციაზე, რომელსაც მომხმარებელი შეიტანს ამ სისტემებში

რეგისტრაციის დროს. ამიტომ საჭირო მომხმარებლის ელექტრონული მისამართის მოძებნა ძალზე რთულია.

ალტერნატიული ძებნის მეთოდით რეკომენდირებულია ელექტრონული მისამართების ძებნა ტელეკომუნიკაციების მასალების მიხედვით. თუკი შევძლებთ საჭირო ადამიანისგან წერილის მოძებნას, მაშინ მიიღებთ გამოძგზავნის კოორდინატებსაც. ამ პრინციპით მოქმედებენ ზოგიერთი ავტომატიზირებული საძიებო სისტემები.

- <http://www.whothere.com/>
- <http://www.emailbook.com/>
- <http://www.dubna.ru/DB/win/who/who>
- <http://www.yandex.com/>

ინფორმაცია ინტერნეტის შესახებ

- <http://www.w3.org/>

ამ სერვერზე ინახება ინტერნეტის ოფიციალური დოკუმენტები. HTML ენის მოქმედი სტანდარტები და მისი ახალი ვერსიები, მიმართვები კომუნიკაციებზე ინტერნეტის მუშაობის საკითხების ირგვლივ და ა.შ.

- <http://www.bouteil.com/>

სერვერზე განთავსებულია ხშირად დასმული შეკითხვები და პასუხები.

- <http://web.canlink.com/helpdesk/window.html>

HTML რელაქტორების სია კომპანია-დამმუშავებლების WWW-მისამართების მითითებით.

- <http://www.javasoft.com/>

WWW-გვერდების უფასოდ განთავსების მომსახურების სერვერები

- <http://www.haliava.ru/>
- <http://www.geosites.com/>
- <http://www.freeyellow.com/>
- <http://www.vibor.ru/>
- <http://www.glasnet.ru/glasweb/rus/chats.html>

ამ გვერდზე მოცემულია Chat-ის მომსახურების სერვერების სია.

- <http://www.real.com/>

სერვერი მიძღვნილია ინტერნეტით ცოცხალი მუსიკისა და ვიდეოს გადაცემის პრობლემებს. შეიცავს რეკომენდაციებს მათთვის ვისაც სურს ქსელიდან მოუსმინოს რადიოს და უცქიროს ვიდეოს. ჩამოტვირთოს პროგრამების ბოლო ვერსიები.

საფოსტო სერვერები

საფოსტო სერვერები, რომლებიც უზრუნველყოფენ საფოსტო ყუთის გახსნის უფასო მომსახურებას:

- <http://www.hotmail.com/>
- <http://www.rambler.ru/>
- <http://www.posta.ge/> (ქართული)
- <http://www.best.ge/> (ქართული)
- <http://www.mail.ru/>

Windows-ის პროგრამული უზრუნველყოფა

რა თქმა უნდა პირველ რიგში მოვიტანთ კორპორაცია **Microsoft** სერვერს. მასზე თქვენ იპოვით ამ ფირმის პროდუქციის ბოლო სიახლეებს და ჩამოტვირთავთ პროგრამული პროდუქტების სადემონსტრაციო ვერსიებს.

- <http://www.microsoft.com/>

ქართული საძიებო გვერდები

- <http://www.internet.ge/>

■ <http://www.google.ge/>

რასაკვირველია არსებობს უამრავი სერვერები და ინტერნეტის გვერდები მაგ: სათამაშო სერვერები, პრესა, განათლება, და სხვა რომლებიც გვთავაზობენ სხვადასხვა სახის მომსახურებას და ინფორმაციას, რომელთა ჩამოთვლა შეუძლებელია ამ წიგნის ფარგლებში.

გამომცემელი: შიდა ქართლის საერო უნივერსიტეტის
კომპიუტერული ცენტრი

ცენტრის ხელმძღვანელი: ზაურ (ბაჩო) თეთრუაშვილი

კომპიუტერული უზრუნველყოფა: თეა ფხალაძე

ბირჟი: 500 ეგზემპლარი