

საქართველოს ტექნიკური უნივერსიტეტი

ოთარ შონია, ნინო თოფურია, გიორგი მაისურაძე

ინფორმაციული უსაფრთხოების სისტემების
აბეზა კორპორაცია MICROSOFT-ის ტექნოლოგიების
გამოყენებით

(სახელმძღვანელო)

თბილისი – 2009

სახელმძღვანელოში წარმოდგენილია ის მეთოდები და ინსტრუმენტები, რომლებიც უზრუნველყოფენ უსაფრთხო მუშაობის წესებს Ms Windows-ს გარემოში. კერძოდ, განხილულია რეგისტრაციისა და აუტენტიფიკაციის წესები, აღრიცხვის ჩანაწერები და პაროლები, უსაფრთხოების ჯგუფები, ფაილების უსაფრთხოების დაცვა NTFS ფორმატის გამოყენებით, სერტიფიკატები, კოდირებული შეტყობინებების ელექტრონული ფოსტით გაგზავნის საშუალებები, მოვლენათა აუდიტი და ელექტრონულ ფოსტასთან უსაფრთხო მუშაობის წესები.

სახელმძღვანელო განკუთვნილია ინფორმატიკის სპეციალობის სტუდენტებისათვის. აგრეთვე შეიძლება გამოიყენონ მაგისტრანტებმა და მეცნიერ მუშაკებმა.

რეცენზენტი: საქართველოს მეცნიერებათა ეროვნული აკადემიის წევრ კორესპონდენტი გ.გოგიჩაიშვილი

სარჩევნი

თავი 1. უსაფრთხოების ინფრასტრუქტურა.....	5
1.1. აღრიცხვის ჩანაწერები.....	5
1.2. უსაფრთხოების ჯგუფები.....	6
1.3. მომხმარებელთა აღრიცხვის ჩანაწერების შექმნა.....	7
1.4. აღრიცხვის ჩანაწერების გამორთვა/წაშლა	9
1.5 მომხმარებელთა აღრიცხვის ჩანაწერების ჩართვა უსაფრთხოების ჯგუფებში	11
1.6. აღრიცხვის ჩანაწერების მართვის საშუალებები	13
1.7. მომხმარებელთა პაროლები	16
1.8. პაროლების პოლიტის დაყენება და გამოყენება.....	17
1.9. Password Reset Disk-ის გამოყენება.....	19
1.10. დაცვა Welcome ეკრანის საშუალებით	20
1.11. უსაფრთხოების უზრუნველყოფა კლასიკური სცენარით რეგისტრაციისას.....	21
1.13. გამაფრთხილებელი შეტყობინება.....	22
1.14. დაცვის დამატებითი დონე (თვისება Syskey)	23
1.15. უსაფრთხოების წესები მომხმარებელთა აღრიცხვის ჩანაწერებისა და პაროლებისათვის	24
თავი 2. უსაფრთხოების დაცვის ძირითადი პრინციპები.....	26
2.1. NTFS ფორმატის გამოყენება ფაილებისა და საქალაქების სამართავად.....	26
2.2. პირად დოკუმენტებთან მიმართვის ბლოკირება	29
2.3. როგორ მივმართოთ ფაილს თუ არ გვაქვს მიმართვის უფლება	30
2.4. პროგრამებთან მიმართვის ფორმირება ბრძანებათა სტრიქონიდან.....	31
2.5. პროგრამებთან მიმართვის შეზღუდვა	33
2.6. პერიფერიული მოწყობილობების მართვა	33
თავი 3. უსაფრთხო ინტერნეტი და ელექტრონული ზონა.....	35
3.1. ვირუსები და მათთან ბრძოლა.....	35

3.2. უსაფრთხოების ზონები	41
3.3. ციფრული სერთიფიკატები	43
3.4. ელექტრონული ფოსტის დაცვა S/MIME-ის საშუალებით	51
3.5. ინფორმაციის დაშიფრვა PGP-ის საშუალებით	53
3.6. დაშიფრვის სხვა საშუალებები	59
თავი 4.0.4. ვაილდისა და საქალაქების კოდირება	62
4.1. მონაცემების კოდირება	62
4.2. მონაცემების აღდგენის აგენტის დანიშვნა	66
4.3. სერთიფიკატების სარეზერო კოპირება	70
თავი 5.0. მონაცემების დაცვა	73
5.1. მონაცემთა სარეზერო ასლების შექმნა	73
5.2. მონაცემთა დაცვის სხვა საშუალებები	77
5.3. უსაფრთხოების მდგომარეობის შემოწმება MBSA უტალიტით	81
თავი 6.0. მოვლენათა მონიტორინგი უსაფრთხოების სისტემაში	84
6.1. მოვლენათა აუდიტი	84
6.2. ფაილებთან და პრინტერებთან მიმართვის უსაფრთხოების აუდიტის კონფიგურირება	86
6.3. უსაფრთხოების ჟურნალის დათვალიერება	90
6.4. ჟურნალების ფაილების დამუშავება	92
თავი 7.0. ჯგუფური პოლიტიკები	94
7.1. უსაფრთხოების უზრუნველყოფასთან დაკავშირებული პოლიტიკები	94
7.2. მომხმარებლის მიმართვის უფლება	95
7.3. უსაფრთხოების უზრუნველყოფის პარამეტრები	96
7.4. ჯგუფური პოლიტიკები	99
7.5. სხვადასხვა მიმართვის უფლებები განსხვავებული მომხმარებლებისათვის	107

თავი 1. უსაფრთხოების ინფრასტრუქტურა

1.1. აღრიცხვის ჩანაწერები

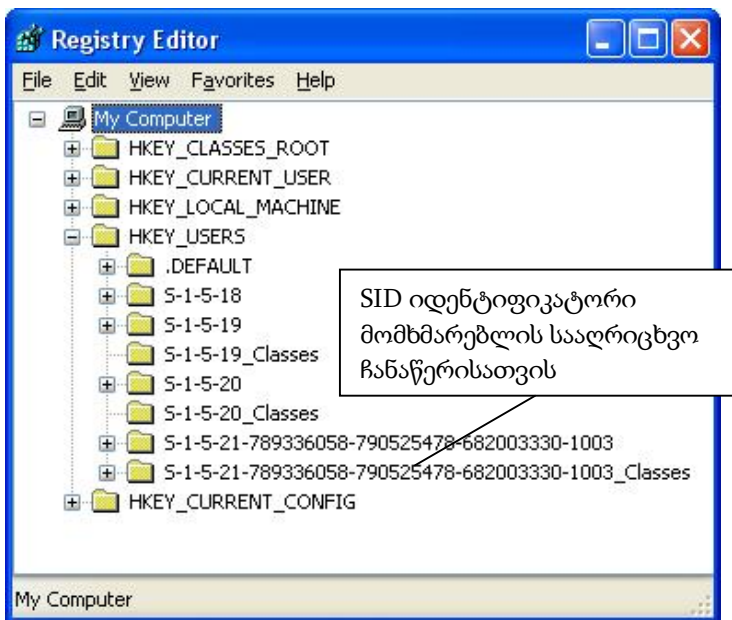
Windows XP-ში არსებობს სისტემური კომპონენტებისა და ინსტრუმენტების ფართო არჩევანი, რომელთა სწორად გამოყენებაც თქვენი კომპიუტერის უსაფრთხო მუშაობას უზრუნველყოფს.

ძირითადი ადგილი ამ ინფრასტრუქტურაში მომხმარებელთა აღრიცხვის (User Accounts) ჩანაწერებს ეკუთვნის. თითოეული კომპიუტერის მომხმარებელს რეგისტრაციის პროცესში ენიჭება საკუთარი აღრიცხვის ჩანაწერი, რომელთა დაცვაც შეიძლება პაროლით. ასეთი საშუალებით მომხმარებლებს შეუძლიათ მიმართონ ფაილებს, საქაღალდეებს, პრინტერს, სხვა რესურსებს და რაც მნიშვნელოვანია ამ საშუალებით კომპიუტერი დაბლოკილია სხვა მომხმარებლებისთვის.

მიუხედავად იმისა, რომ რეგისტრაციის პროცესი მეტად მარტივია მას ახასიათებს გარკვეული თავისებურებანი. სისტემური ადმინისტრატორის შესაძლებლობები იცვლება Windows-ის ვერსიებთან ერთად, ასევე ბევრია დამოკიდებული Windows-ის ინსტალაციის დროს ამორჩეულ ოფიცებზე.

ინფორმაცია მომხმარებელთა აღრიცხვის ჩანაწერების შესახებ ინახება დაცულ მონაცემთა ბაზაში Security Accounts Manager (SAM). მომხმარებლის აღრიცხვის ჩანაწერის შექმნის მომენტში მას მიენიჭება უნიკალური SID იდენტიფიკატორი. SID-ის ყველა მნიშვნელობა იწყება S-1 სიმბოლოებით, ხოლო შემდეგ მოდის რიცხვების მიმდევრობა, რომელიც უნიკალურად განსაზღვრავს აღრიცხვის ჩანაწერს. ამ იდენტიფიკატორთან მიმართვა შესაძლებელია სისტემური რეგისტრის საშუალებით (regedit).

SID იდენტიფიკატორი შექმნა ხდება მომხმარებლის ახალი აღრიცხვის ჩანაწერის შექმნის თანავე და არსებობს მისი წაშლის მომენტამდე. თუ ამავე მომხმარებლისა და პაროლისთვის შექმნით ახალ აღრიცხვის ჩანაწერს, მას მიენიჭება ახალი SID-იდენტიფიკატორი. იხილეთ ნახ.1.1. SID-ის შესახებ დაწვრილებით ინფორმაციის მისაღებად მიმართეთ შემდეგ საიტებს: http://www.microsoft.com/teachnet/ptodtechnol/winxppro/reskit/prnc_cid_cids.asp.



ნახ.1.1

1.2. უსაფრთხოების ჯგუფები

უსაფრთხოების ჯგუფები, წარმოადგენენ მომხმარებელთა აღრიცხვის ჩანაწერების კოლექციას, რომლებიც უსაფრთხოების სისტემის ადმინისტრირების საშუალებას იძლევიან. ასეთი ჯგუფების გამოყენება მნიშვნელოვნად ამარტივებს მუშაობას, რადგანაც ერთნაირი მიმართვის უფლებების მქონე მომხმარებელთა აღრიცხვის ჩანაწერებს აქვთ პრივილეგიების იდენტური ნაკრები.

Windows-ის შემადგენლობაში შედის ცხრა ჩაშენებული ჯგუფი, ასევე დასაშვებია დამატებითი ჯგუფების შექმნაც.

Administrators (ადმინისტრატორები) – ესაა ყველაზე მძლავრი ჯგუფი, რომელსაც უფლება აქვს სრულად აკონტროლოს სისტემა.

Power Users (გამოცდილი მომხმარებლები) – აქვთ მრავალი პრივილეგია, მაგრამ არა იმდენი რაც ადმინისტრატორს.

Users (მომხმარებლები) – ესაა შეზღუდული უფლებების ნაკრები ისეთი მომხმარებლებისათვის, რომელთაც არ ეძლევათ სისტემის ადმინისტრირების უფლება.

Guests (სტუმრები) – ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლებები განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის.

Backup Operators (სარეზერვო ასლის შექმნის ოპერატორები) – იმ პრივილეგიების მინიჭება, რომელიც საჭიროა ფაილების, საქაღალდეების რეზერვირებისა და აღდგენისათვის.

Replicator (რეპლიკატორი) – უზრუნველყოფს რეპლიკაციების მართვას დომენურ ქსელებში.

Network Configuration Operators (ქსელის კონფიგურირების ოპერატორები) – ამ ჯგუფის წევრებს აქვთ ქსელური კომპონენტების კონფიგურირებისა და დაყენების უფლება.

Remote Desktop Users (დაშორებული მომხმარებლები) – კომპიუტერთან მიმართვის უზრუნველყოფა Remote Desktop Connection-ის საშუალებით.

Help Services Group (ტექნომხსახურების ჯგუფები) – რათა ტექნიკურ პერსონალს მიეცეს საშუალება მიუერთდეს კომპიუტერს.

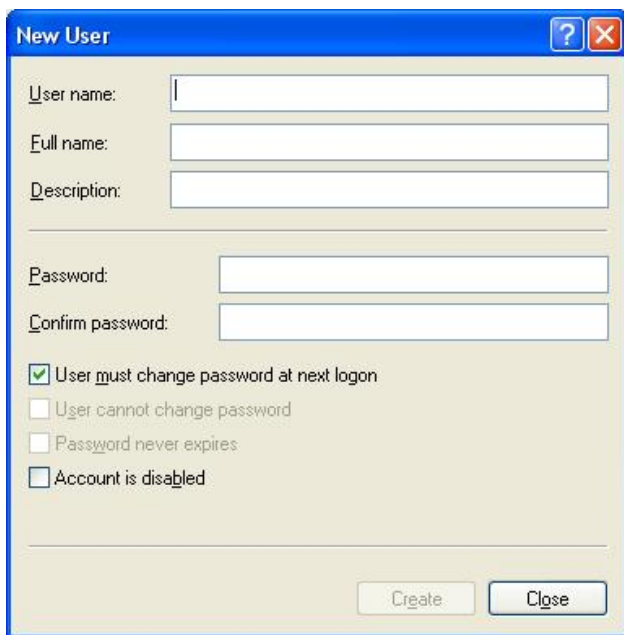
1.3. მომხმარებელთა აღრიცხვის ჩანაწერების შექმნა

მომხმარებელთა აღრიცხვის ჩანაწერების შექმნა შეიძლება ოთხი გზით:

– უტილიტა Users and Passwords, აირჩიეთ ღილაკი Users, შემდეგ ღილაკი Add. გამოჩნდება ოსტატი, სადაც აირჩიეთ მომხმარებლის სახელსა და პაროლს. აქ ასევე შესაძლებელია აღრიცხვის ჩანაწერის დამატება უსაფრთხოების ლოკალურ ჯგუფში.

– უტილიტა Local Users and Groups. აირჩიეთ საქაღალდე Users, მისი კონტექსტური მენიუდან აირჩიეთ ბრძანება New User. მიუთითეთ მონაცემები New User-ის შესახებ და დააჭირეთ კლავიშას Create. იხილეთ ნახ.1.2.

– უტილიტა User Accounts-ის საშუალებით, აღრიცხვის ჩანაწერი იქმნება ღილაკით Create New Account. აქვე უნდა განისაზღვროს მივანიჭოთ აღრიცხვის ჩანაწერს ადმინისტრატორის უფლებები, თუ დავაღოთ შეზღუდვები.



ნახ.1.2

– ბრძანება Net User. ბრძანების შესასრულებლად Command Prompt ფანჯარაში აკრიფეთ ბრძანება:

Net User მომხმარებლის სახელი / Add / random

ცხრილში მოცემულია Net User ბრძანებათა პარამეტრები

პარამეტრი	აღწერა
/Add	ახალი აღრიცხვის ჩანაწერის შექმნა. მომხმარებლის სახელი შეიძლება შეიცავდეს მაქსიმუმ 20 სიმბოლოს, აკრძალულია „/ \ [] ; = , + * ? < >“ სიმბოლოების გამოყენება.
პაროლი,* /Random	პაროლის დაყენება. თუ მიუთითებთ (*), ეკრანზე გამოჩნდება შეტყობინება მომხმარებლის პაროლის შეტანის შესახებ. /Random-ის მითითების შემთხვევაში პაროლი გენერირდება შემთხვევითი წესით და შედგება 8 სიმბოლოსაგან.

/Fullname: ”სახელი”	მომხმარებლის სრული სახელის მითითება.
/Comment:” ტექსტი”	აღწერითი კომენტარის მითითება.
/Passwordchg: yes ან Passwordchg: no	მომხმარებლისათვის პაროლის შეცვლის უფლების მინიჭება.
/Active:no ან /Active:yes	აღრიცხვის ჩანაწერის აქტივიზაცია/ ბლოკირება.

1.4. აღრიცხვის ჩანაწერების გამორთვა/წაშლა

იმ შემთხვევაში, როდესაც აღრიცხვის ჩანაწერები აღარ არის საჭირო იგი ან უნდა გამოვრთოთ ან წაშალოთ. აღრიცხვის ჩანაწერების გამორთვის შემთხვევაში მომხმარებლები რეგისტრაციაზე არ დაიშვებიან, თუმცა ხელუხლებელი რჩება მათი აღრიცხვის ინფორმაცია, სერტიფიკატები და მომხმარებელთა ფაილები. თუ აღრიცხვის ინფორმაცია დაგვჭირდება შემდგომში, ხდება მისი გააქტიურება, თუ იგი აღარ არის საჭირო, უმჯობესია მისი წაშლა.

აღრიცხვის ჩანაწერის გამოსართავად არსებობს შემდეგი მეთოდები:

- უტილიტა Local Users And Groups ფანჯარაში, აირჩიეთ საჭირო აღრიცხვის ჩანაწერი. ეკრანზე გამოსულ დიალოგიურ ფანჯარაში აირჩიეთ ლილაკი General. ჩართეთ/გამორთეთ ოფცია Accounts is Disables.

- Command Prompt ფანჯარაში აღრიცხვის ჩანაწერის გამოსართველად აკრიფეთ ბრძანება:

net user მომხმარებლის სახელი/ active :no

ჩასართავად აკრიფეთ ბრძანება:

net user მომხმარებლის სახელი/ active :yes

აღრიცხვის ჩანაწერის წაშლის შემთხვევაში მისი გამოყენება შეუძლებელია. ამასთან, შეუძლებელია რესურსებთან ძველი მიმართვების აღდგენა აღრიცხვის ჩანაწერის ხელმეორედ შექმნის შემთხვევაში. რესურსებში იგულისხმება მომხმარებელთა კოდირებული

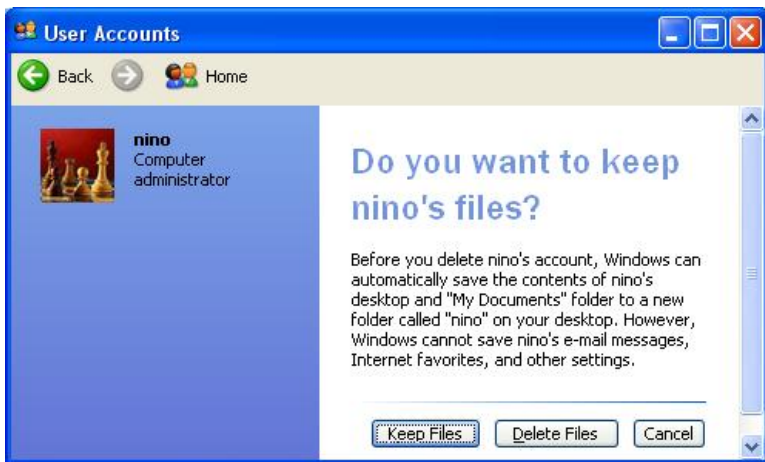
ფაილები, პერსონალური სერთიფიკატები, ასევე ის პაროლები, რომლებიც განკუთვნილი იყო ვებ-კვანძებთან და სხვა ქსელურ ინფორმაციასთან მიმართებისათვის. საქმე იმაშია, რომ მიმართვის უფლებები დაკავშირებულია SID აღრიცხვის ჩანაწერებზე. ახალი აღრიცხვის ჩანაწერის შექმნისას (იმ შემთხვევაშიც კი, თუ მომხმარებლის სახელი და პაროლი ემთხვევა უკვე წაშლილ აღრიცხვის ჩანაწერს) ხდება SID იდენტიფიკატორის გენერაცია, ამიტომ, ახალი აღრიცხვის ჩანაწერის უფლებები განსხვავდება წინა აღრიცხვის ჩანაწერის უფლებებისაგან.

დასაშვებია ნებისმიერი აღრიცხვის ჩანაწერის წაშლა (გარდა Administrator-ისა და Guest-ისა ან იმ აღრიცხვისთვის ჩანაწერისა, რომელთანაც მიერთებული ხართ ამჟამად).

– უტილიტა Users and Passwords გააქტიურებისას, აირჩიეთ ჩანართი Users, აირჩიეთ წასაშლელი აღრიცხვის ჩანაწერი და დაჭირეთ ღილაკს Remove.

– უტილიტა Local Users And Groups ფანჯარაში, აირჩიეთ ღილაკი Users, ეკრანზე გამოჩნდება მომხმარებელთა სია. აირჩიეთ საჭირო აღრიცხვის ჩანაწერი და მისი კონტექსტური მენიუდან აირჩიეთ Delete.

– უტილიტა User Accounts გააქტიურებისას, აირჩიეთ წასაშლელი აღრიცხვის ჩანაწერი. აირჩიეთ Delete The Accounts. ეკრანზე გამოჩნდება დიალოგიური ფანჯარა. იხილეთ ნახ.1.3.



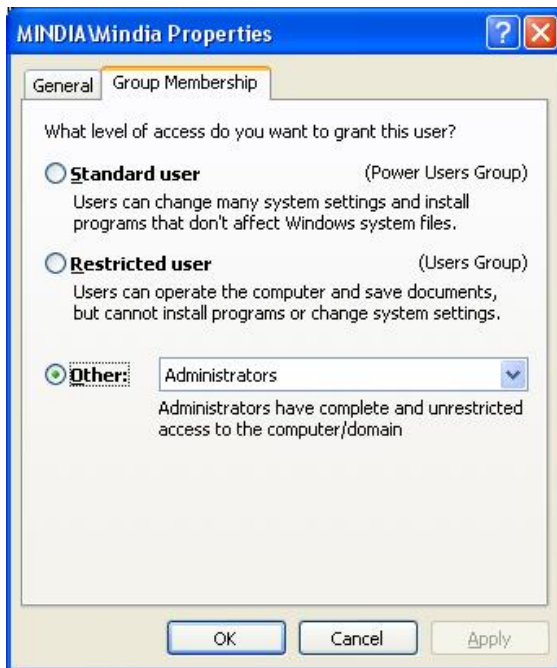
ნახ.1.3

ოფცია Keep Files-არჩევისას, მოხდება მომხმარებელთა ფაილებისა და საქალაქების, რომლებიც მდებარეობენ სამუშაო მაგიდაზე და My Documents საქალაქში, კოპირება სპეციალურ საქალაქში სამუშაო მაგიდაზე.

ოფცია Delete Files – არჩევისას, ჩაიშლება მიმდინარე აღრიცხვების ჩანაწერი და მასთან დაკავშირებული ყველა ფაილი.
– ბრძანება New User მომხმარებლის სახელი/ Delete.

1.5 მომხმარებელთა აღრიცხვის ჩანაწერების ჩართვა უსაფრთხოების ჯგუფებში

თუ კომპიუტერის მომხმარებელთა სია მკაცრად კონტროლირდება, საჭიროა თითოეული მომხმარებელი ჩართოთ ცალკეულ უსაფრთხოების ჯგუფებში. უსაფრთხოების ჯგუფებისათვის დადგენილია გარკვეული მიმართვის წესები და უფლებები, რომლებიც მისაღებია მომხმარებელთა უმრავლესობისათვის.

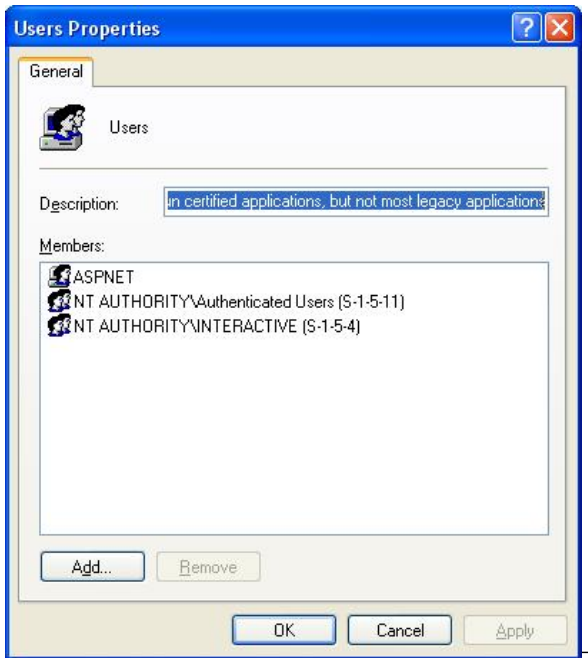


ნახ.1.4

– უტილიტა Users and Passwords გააქტიურებისას, მოიშნეთ ჩანართი Users. აირჩიეთ აღრიცხვის ჩანაწერი (თაგუს მარცხენა ღილაკს დააჭირეთ 2-ჯერ), დააჭირეთ ღილაკს Group Membership, და აირჩიეთ უსაფრთხოების ჯგუფი. იხილეთ ნახ.1.4.

უტილიტა Local Users and Group ჯგუფებში გაწვევრიანების მართვის საუკეთესო მეთოდებს იძლევა:

– კონკრეტული მომხმარებლის ჯგუფებში გაერთიანების სამართავად კონსოლის ხეზე აირჩიეთ Users, აირჩიეთ მომხმარებელი (თაგუს მარცხენა ღილაკს დააჭირეთ 2-ჯერ), შემდეგ აირჩიეთ ჩანართი Member of, შემდეგ ღილაკი Add და შეავსეთ დიალოგიური ფანჯარა. ღილაკით Remove შეიძლება მომხმარებლის აღრიცხვის ჩანაწერის ამოღება ჯგუფიდან.



ნახ.1.5

ჯგუფებში გაწვევრიანებისათვის აირჩიეთ ღილაკი Groups. კონსოლის ხეზე გამოჩნდება ჯგუფების ჩამონათვალი. ამა თუ იმ ჯგუფის დასახელებაზე თაგუს მარცხენა ღილაკს ორჯერ დაჭერით,

მოსდება ჯგუფში შემავალი წევრების სიის ეკრანზე გამოტანა. ღილაკით Add შესაძლებელია მომხმარებლის აღრიცხვის ჩანაწერის დამატება ჯგუფში, ხოლო ღილაკით Remove მომხმარებლის აღრიცხვის ჩანაწერის ამოღება ჯგუფიდან. იხილეთ ნახ.1.5.

– უტილიტა Users Accounts საშუალებას იძლევა აღრიცხვის ჩანაწერი გაერთიანდეს მხოლოდ და მხოლოდ Administrators და Users-ს ჯგუფებში. ცვლილებების განსახორციელებლად აირჩიეთ Change the Account Type.

1.6. აღრიცხვის ჩანაწერების მართვის საშუალებები

უტილიტა Users and Passwords

მისი საშუალებით შესაძლებელია შემდეგი მოქმედებების შესრულება:

- შეცვალოთ მომხმარებელთა აღრიცხვის ჩანაწერები.
- მოახდინოთ ავტომატური რეგისტრაციის კონფიგურირება.
- Ctrl+Alt+Del კლავიშების კომბინაციის დაყენება.

უტილიტის გასააქტიურებლად ბრძანებათა სტრიქონში აკრიფეთ control userpasswords2. იხილეთ ნახ.1.6.

უტილიტა Local Users and Groups

ამ უტილიტასთან მიმართვა ხორციელდება კონსოლით Microsoft Management Console (MMC). იხილეთ ნახ.1.7. აქ არსებობს გაცილებით მეტი შესაძლებლობა ვიდრე Users and Passwords უტილიტის შემთხვევაში. ამ უტილიტის გააქტიურება შესაძლებელია შემდეგი ხერხებით:

- 1) აირჩიეთ ბრძანება:
Administrative Tools → Computer Management → System Tools
→ Local Users and Groups.
- 2) ბრძანებათა სტრიქონში აკრიფეთ ბრძანება: `lusrmgr.msc`
- 3) უტილიტა Users and Passwords-ის ფანჯარაში აირჩიეთ ოფცია Advanced.



ნახ.1.6

Net-ბრძანებები

ბრძანებათა სტრიქონის ეს უტილიტებია Net User და Net Localgroup. დამატებითი ცნობების მისაღებად აკრიფეთ

ჩამონათვალის და სინტაქსის დასათვალისებლად აკრიფეთ ბრძანებები net user/? და net localgroup/?.

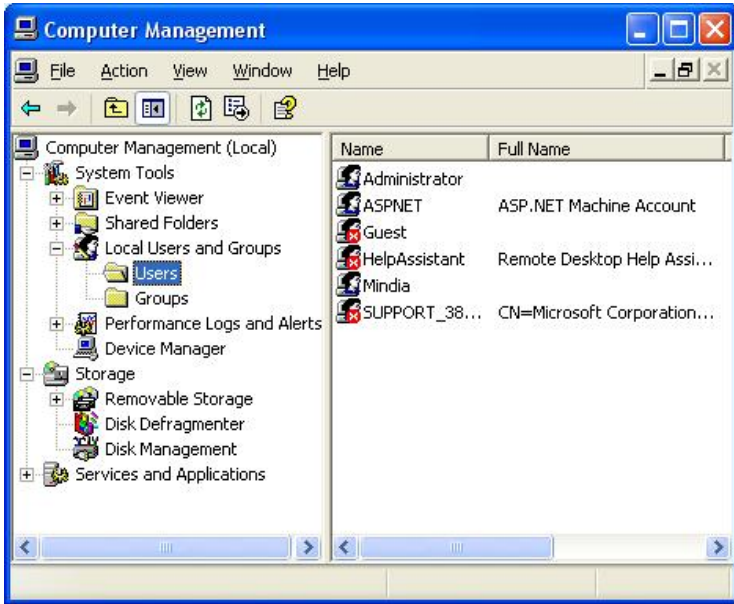
Net-ბრძანების შესრულება მოსახერხებელია Command Prompt ფანჯარაში, რისთვისაც Run ბრძანებათა სტრიქონში აკრიბეთ cmd.

უტილიტა Users Accounts

ამ უტილიტის გასააქტიურებლად აირჩიეთ ბრძანება:

Control Panel → User Accounts

ცხრილში განხილულია აღრიცხვის ჩანაწერების მართვის საშუალებების ფუნქციები:



ნახ.1.7

ამოცანა		Users And Passwords	Local Users And Groups	Net-ბრძანებები	User Accounts
აღრიცხვის შექმნა	ჩანაწერის	ღიას	ღიას	ღიას	ღიას
აღრიცხვის წაშლა	ჩანაწერის	ღიას	ღიას	ღიას	ღიას
აღრიცხვის ჩართვა	ჩანაწერის უსაფრთხოების ჯგუფში	ღიას	ღიას	ღიას	ღიას
მომხმარებლის შეცვლა	სახელის	ღიას	ღიას	არა	არა
პაროლის დაყენება		ღიას	ღიას	ღიას	ღიას
პაროლის დაყენება	კარნახის	არა	არა	არა	არა

აღრიცხვ აქტივიზაცია/გამორთვა	ჩანაწერის	არა	დიახ	დიახ	დიახ
საღრიცხვო ბლოკირების მოხსნა	ჩანაწერზე	არა	დიახ	დიახ	არა

1.7. მომხმარებელთა პაროლები

უსაფრთხოების დაცვის მიზნით თითოეულ აღრიცხვის ჩანაწერს აუცილებელია ჰქონდეს თავისი რეგისტრაციის პაროლი. პაროლის დანიშვნა ხდება შემდეგი უტილიტებით.

– უტილიტა Users and Passwords, აირჩიეთ ჩანართი Users, მომხმარებლის სახელი და ლილაკი Reset Password.

– უტილიტა Local Users and Groups. აირჩიეთ საქალაღე Users, მომხმარებლის სახელი, შემდეგ დააჭირეთ თავუს მარჯვენა ლილაკს და აირჩიეთ ოფცია Set Password.

– უტილიტა Users Accounts. აირჩიეთ მომხმარებლის აღრიცხვის ჩანაწერი და ლილაკი Create A Password. აქვე შეიღლება პაროლისათვის კარნახის ფორმირება.

– პაროლის დაყენება შესაძლებელია ბრძანებით Net User. Command Prompt რეჟიმში აკრიფეთ შემდეგი ბრძანება:

Net User მომხმარებლის სახელი პაროლი

სადაც პარამეტრი პაროლი ღებულობს შემდეგი სამი მნიშვნელობიდან ერთ-ერთს.

– დასანიშნი პაროლი;
– * (ამ შემთხვევაში მომხმარებელს ეძლევა საშუალება თვითონ მიუთითოს პაროლი)

– / random (Windows-ი თვითონ ახდენს რთული პაროლის გენერირებას, რომელიც რვა სიმბოლოსაგან შედგება)

სასურველია, პაროლი იყოს რთული, რათა პაროლების „გატეხვის“ პროგრამას გაუჭირდეს მისი ამოცნობა. ასევე, სასურველია რთული პაროლის ხშირი განახლება.

რთული პაროლის მახასიათებლებია:

- შეიცავდეს მინიმუმ რვა სიმბოლოს
- შედგებოდეს ზედა/ქვედა რეგისტრის ასოებისაგან, სიმბოლოებისა და ციფრებისაგან;

- პერიოდულად შეიცვალოს პაროლი; ამასთან ახალი მნიშვნელოვნად უნდა განსხვავებოდეს ძველი პაროლისაგან.
- არ უნდა შეიცავდეს სახელებს, მომხმარებლის სახელებს, ან რომელიმე აზრიან სიტყვებს.
- რთული პაროლები დასამახსოვრებლად ძნელია. ეფექტური მიდგომა იმაში მდგომარეობს, რომ ადვილად დასამახსოვრებელი ფრაზა გადავაკეთოთ ძნელად ამოსაცნობ პაროლად. მაგალითად, ფრაზა „Windows XP Security“ და დაბადების დღე „18 იანვარი“ (18-1) მივიღებთ პაროლს 18WXP-1.

1.8. პაროლების პოლიტიკის დაყენება და გამოყენება

პაროლების პოლიტიკის დაყენება ხდება კონსოლიდან Local Security Settings, მის გასააქტიურებლად ბრძანების სტრიქონში აკრიფეთ secpol.msc. იმ პოლიტიკების სანახავად, საიდანაც ხდება „ქცევის წესების“ განსაზღვრა თითოეული აღრიცხვის ჩანაწერისათვის, გასხენით ფანჯარა Security Settings → Account Policies → Password Policy. არსებობს მეორე გზაც, აირჩიეთ შემდეგი ბრძანება:

Administrative Tools → Local Security Policy

ცხრილში ქვემოთ განმარტებულია თითოეული პოლიტიკა:

პოლიტიკა	აღწერა
ავსახოთ პაროლების ქრონოლოგია	დადებითი რიცხვი (მაქ. 24). Windows-ი იმახსოვრებს წინა პაროლების რაოდენობას და მიუთითებს მომხმარებელს გამოიყენოს ისეთი პაროლი, რომელიც განსხვავდება წინა პაროლებისაგან.
პაროლების მოქმედების	დადებითი რიცხვი (მაქს.999) მიუთითებს დღეების რაოდენობას, რომელთა განმავლობაშიც პაროლი „ვარგისია“. „0“ ნიშნავს, რომ პაროლი არასდროს არ ძველდება.

<p>მაქსიმალური ვადა</p>	<p>დადებითი რიცხვი (მაქ.999), რომელიც განსაზღვრავს ვადას, როდესაც მომხმარებელს ეძლევა საშუალება შეცვალოს იგი. „0“ ნიშნავს, რომ პაროლის შეცვლა შეიძლება ნებისმიერ დროს.</p>
<p>პაროლის მოქმედების</p>	<p>დადებითი რიცხვი (მაქ.14) განსაზღვრავს, პაროლის შემადგენელი სიმბოლოების რაოდენობას. „0“ მიუთითებს, რომ მომხმარებელი უარს ამბობს პაროლებზე. ცვლილებების შეტანა არ რეაგირებს მიმდინარე პაროლებზე.</p>
<p>მინიმალური ვადა</p>	<p>გააქტიურებს პოლიტიკას, რომლის თანახმად ახალი პაროლი უნდა შეადგენდეს მინიმუმ 6 სიმბოლოს; პაროლი უნდა შედგებოდეს ორივე რეგისტრის სიმბოლოსაგან და რიცხვებისაგან. არ უნდა შეიცავდეს მომხმარებლის სახელს.</p>
<p>პაროლის მინიმალური სიგრძე</p>	<p>გააქტიურებს პოლიტიკას, რომლის თანახმადაც პაროლები შეიძლება ინახებოდეს ჩვეულებრივი ტექსტის სახით. ეს პოლიტიკა საჭიროა მოძველებულ პროგრამებთან მუშაობის თავისებურების გასათვალისწინებლად.</p>

ასევე არსებობს აღრიცხვის ჩანაწერების ბლოკირების საშუალებებიც, რისთვისაც საჭიროა აირჩიოთ ბრძანება: Run → Secpol.msc → Security setting → Account Policies → Account Lockout policy.

აღრიცხვის ჩანაწერების ბლოკირების პოლიტიკები აღწერილია ცხრილში:

პოლიტიკა	აღწერა
<p>აღრიცხვის ჩანაწერების ბლოკირების ხანგძლივობა</p>	<p>დადებითი რიცხვი (მაკ.99999 წთ), რომელიც მიუთითებს აღრიცხვის ჩანაწერების ბლოკირების ხანგძლივობაზე. მითითებული დროის გასვლის შემდეგ აღრიცხვის ჩანაწერებზე მოიხსნება ბლოკირება. თუ მითითებულია „0“, აღრიცხვის ჩანაწერი დაიბლოკება სამუდამოდ და საჭირო გახდება ადმინისტრატორის ჩარევა.</p>
<p>აღრიცხვის ჩანაწერების ბლოკირების ზღურბლი</p>	<p>დადებითი რიცხვი (მაკ.99999) რომელიც განსაზღვრავს პაროლების შერჩევის ცდების რაოდენობას დროის მოცემულ შუალედში.</p>
<p>აღრიცხვის ჩანაწერის ბლოკირების მრიცხველის გადაყენება</p>	<p>დროის ინტერვალის მითითება (99999წთ), რომლის განმავლობაშიც ხდება აღრიცხვის ჩანაწერის ბლოკირება, პაროლების შერჩევის გარკვეული რაოდენობის ცდების შემდეგ.</p>

1.9. Password Reset Disk-ის გამოყენება

Password Reset Disk-ის ჩვეულებრივი დისკია, რომელიც შესაძლებელია მომხმარებელთა რეგისტრაცია პაროლის აკრების გარეშე. ასეთი დისკის შესაქმნელად აუცილებელია მიმდინარე პაროლის ცოდნა, წინააღმდეგ შემთხვევაში ნებისმიერ პირს შეუძლია იგივე პროცედურის შესრულება თქვენს მაგიერ.

Password Reset Disk-ის შესაქმნელად საჭიროა შემდეგი მოქმედებების შესრულება:

1. დარეგისტრირდით თქვენი აღრიცხვის ჩანაწერით;
2. აირჩიეთ ბრძანება Control Panel→ User Accounts;
3. აირჩიეთ თქვენი აღრიცხვის ჩანაწერი;
4. აირჩიეთ ელემენტი Prevent A Forgotten Password.



ნახ.1.8

1.10. დაცვა Welcome ეკრანის საშუალებით

ეკრანი Welcome მოხერხებულია მუშაობისას; მომხმარებლებს შეუძლიათ დარეგისტრირდნენ თავიანთს ღილაკს დაჭერით ან პაროლის მითითების შედეგად (თუ მას მოითხოვს აღრიცხვის ჩანაწერი). ეს ეკრანი ასევე ასახავს მომხმარებელთა სახელებს და პაროლების კარნახებს. Welcome ეკრანის გათიშვა ხდება შემდეგნაირად:

1. აირჩიეთ ბრძანება Control Panel→User Accounts→Change The Way Users Log On Or Off.

2. გათიშეთ ალაბი Use The Welcome Screen და აირჩიეთ ღილაკი Apply Options.

ეკრან Welcome-ის გათიშვის შემდეგ ხდება გადასვლა რეგისტრაციის კლასიკურ სცენარზე, როდესაც გააქტიურდება დიალოგიური ფანჯრები Welcome To Windows და log on to Windows. ეკრან Welcome-ის გათიშვის შედეგად ავტომატურად

გაითიშება თვისება Fast User Switching, რომელიც სხვა აღრიცხვის ჩანაწერთ რეგისტრაციის საშუალებას იძლევა. ეს ოფცია უზრუნველყოფს რამოდენიმე მომხმარებლის ერთდროულ რეგისტრაციას.

1.11. უსაფრთხოების უზრუნველყოფა კლასიკური სცენარით რეგისტრაციისას

კლასიკური სცენარით რეგისტრაცია, ითვალისწინებს Ctrl+Alt+Delete კლავიშების კომბინაციას. ამ შემთხვევაში მომხმარებელმა უნდა აკრიფოს მოხმარებლის სახელი და პაროლი. აღნიშნული პროცესის გასააქტიურებლად საჭიროა:



ნახ.1.9

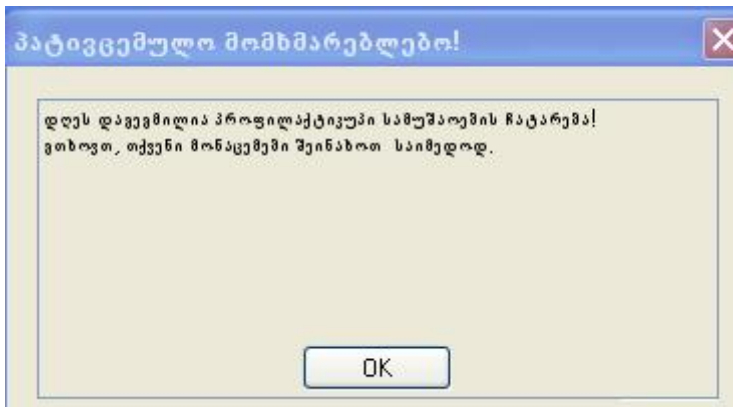
1. აირჩიოთ ბრძანება Run→control userpasswords2.
2. აირჩიოთ ჩანართი Advanced და ჩართეთ ალაში Require Users To Press Ctrl+Alt+Delete იხილეთ ნახ.1.9.

3. ავტონომიური რეგისტრაციის გამორთვისათვის აირჩიეთ ჩანართი Users და ჩართეთ ალაბი Users Must Enter A User Name and Password.

4.

1.13. გამაფრთხილებელი შეტყობინება

არსებობს შემთხვევები, როდესაც საჭიროა მისაღმების ან გამაფრთხილების ტექსტის გამოტანა ეკრანზე. ამ დროს მომხმარებლისათვის განკუთვნილი ტექსტი გამოჩნდება ეკრანზე დაილოგიური ფანჯრის Log On To Windows-ის გამორჩენამდე. იხილეთ ნახ.1.10.



ნახ.1.10

მსგავსი სახის შეტყობინების გამოსატანად საჭიროა:

1. აირჩიეთ ბრძანება Run→Secpol.msc.
2. დაილოგიურ ფანჯარაში აირჩიეთ ბრძანება Security setting → Local Policies → Security Options
3. დააჭირეთ თავუს მარცხენა ღილაკს 2-ჯერ პუნქტზე Message Title For Users Attampting to log on (შეტყობინების სათაური).
4. აკრიფეთ ტექსტი, დააჭირეთ ღილაკს OK.
5. დააჭირეთ თავუს მარცხენა ღილაკს 2-ჯერ პუნქტზე Message Text For Attampting Top Log On (შეტყობინების ტექსტი).
6. აკრიფეთ შეტყობინების ტექსტი, დააჭირეთ ღილაკს OK.

1.14. დაცვის დამატებითი დონე (თვისება Syskey)

თვისება Syskey-ის გამოყენების შემთხვევაში, ჩვეულებრივი რეგისტრაციის ეკრანის გამოჩენისათვის საჭირო ხდება პაროლის შეტანა. მოქმედებების თანმიმდევრობა:

1. ბრძანებათა სტრიქონში აკრიფეთ SysKey.

2. ეკრანზე გამოჩნდება დიალოგიური ფანჯარა. აირჩიეთ ლილაკი Update. იხილეთ ნახ.1.11.

დიალოგიურ ფანჯარაში Startup Key აირჩიეთ ერთ-ერთი შემდეგი სამი ოფციიდან. იხილეთ ნახ.1.12.



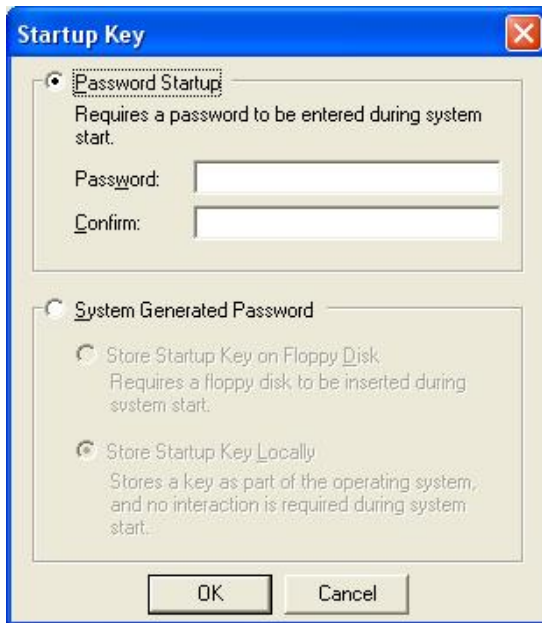
ნახ.1.11

- Password Setup (პაროლის დაყენება). აკრიფეთ პაროლი, რომელიც უნდა აკრიფოს კომპიუტერის ყოველი ჩართვის შედეგად. უსაფრთხოებისათვის უმჯობესია პაროლი შედგებოდეს მინიმუმ 12 სიმბოლოსაგან.
- Store Startup Key Locally (სასტარტო გასაღები შენახულია ლოკალურად. ეს ოფცია ჩართულია „გაჩუმებით“)
- Store Startup Key On Floppy Disk. ამ შემთხვევაში Syskey უტილიტა ახდენს ახალი სასტარტო გასაღების გენერაციას და ინახავს მას დისკეტზე.

1.15. უსაფრთხოების წესები მომხმარებელთა აღრიცხვის ჩანაწერებისა და პაროლებისათვის

ქვემოთ ჩამოთვლილია უსაფრთხოების წესები, რომლებიც საშუალებას იძლევიან დაემალოთ უცხო თვალისაგან აღრიცხვის ჩანაწერები, პაროლები და რეგისტრაციის პროცესის დეტალები.

- თითოეული მომხმარებლისათვის შექმენით ცალკე აღრიცხვის ჩანაწერი;
- გამორთეთ ან წაშალეთ აღრიცხვის ჩანაწერები, რომელთაც აღარ იყენებთ;
- ყველა აღრიცხვის ჩანაწერისათვის გამოიყენეთ არატრივიალური პაროლები;



ნახ.1.12

- დაიცავით ადმინისტრატორის აღრიცხვის ჩანაწერები;
- აირჩიეთ პაროლებთან მუშაობის ისეთი პოლიტიკა, რომლებიც საშუალებას აძლევენ მომხმარებლებს ამოირჩიონ ან რეგულარულად შეცვალონ პაროლები;

- უზრუნველყავით დაკარგული პაროლების აღდგენის საშუალებები;
- გამოიყენეთ პაროლებთან უსაფრთხო მუშაობის სპეციალური პროგრამა;
- გამორთეთ საწყისი ეკრანის გამოსვლა რეგისტრაციის პროცესში;
- დააყენეთ Ctrl+Alt+Del კლავიშების კომბინაციის აკრების მოთხოვნა რეგისტრაციის დაწყებამდე;
- ჩართეთ ეკრანის გამოსახულება, რომელიც ამცნობს მომხმარებელს არასაქციონირებული მიმართვის მცდელობის შესახებ;
- გაააქტიურეთ პაროლების ბლოკირების პოლიტიკა, რომელიც პაროლების შერჩევის პროგრამის გაუქმებას ახდენს;
- უმაღლესი დონის უსაფრთხოების აუცილებლობისას უზრუნველყავით სისტემის ჩატვირთვა, მხოლოდ სპეციალური პაროლის ან სხვა დამხმარე საშუალებების აკრების შედეგ.

საკონტროლო კითხვები:

1. რომელი ოთხი ხერხით შეიძლება აღრიცხვის ჩანაწერების შექმნა?
2. როგორ ჩავრთოთ აღრიცხვის ჩანაწერი უსაფრთხოების ჯგუფებში?
3. როგორ გავთიშოთ ავტომატური რეგისტრაციის პროცესი?
4. რის საშუალებას იძლევა თვისება Syskey?
5. როგორ ჩავრთოთ გამაფრთხილებელი შეტყობინება რეგისტრაციის პროცესში?
6. როგორ დავაყენოთ Ctrl+Alt+Delete კლავიშების კომბინაცია რეგისტრაციის პროცესში?
7. რას ნიშნავს დაცვა Welcome ეკრანის საშუალებით?
8. როგორ ჩავრთოთ პაროლების პოლიტიკები?
9. რას გულისხმობს ტერმინი რთული პაროლი?
10. როგორ ჩავრთოთ პოლიტიკა, რომელიც მოითხოვს მომხმარებლის პაროლის შეცვალას ერთ კვირაში?

თავი 2. უსაფრთხოების დაცვის ძირითადი პრინციპები

2.1. NTFS ფორმატის გამოყენება ფაილებისა და საქაღალდეების სამართავად

პრაქტიკულად ყოველთვის, როდესაც ერთ კომპიუტერთან მუშაობს რამდენიმე მომხმარებელი, წარმოიშობა უსაფრთხოებასთან დაკავშირებული პრობლემები. თუ თითოეულ მომხმარებელს აქვს კომპიუტერთან მიმართვის ისეთი უფლებები, რომლებიც შეესაბამება მის კვალიფიკაციის დონეს, უსაფრთხოების ტექნიკასთან დაკავშირებული რისკი შედარებით დაბალია.

ოპერაციული სისტემა Windows XP, რომელიც უშუალოდ გამოიყენებს NTFS მიმართვის წესებს, – ესაა ერთადერთი საშუალება ააწყოთ უსაფრთხო მუშაობა ფაილებთან და საქაღალდეებთან. მეორეს მხრივ, NTFS-თან უშუალო მიმართვა “გაჩუმების” პრინციპით ბლოკირებულია მოხერხებულობის თვალსაზრისით. იმისათვის, რომ ვიქონიოთ NTFS-სთან მიმართვის სრული ნაკრები, გაააქტიურეთ Windows Explorer, აირჩიეთ ბრძანება Tools → Folder Options და გამორთეთ ოფცია Simple File Sharing.

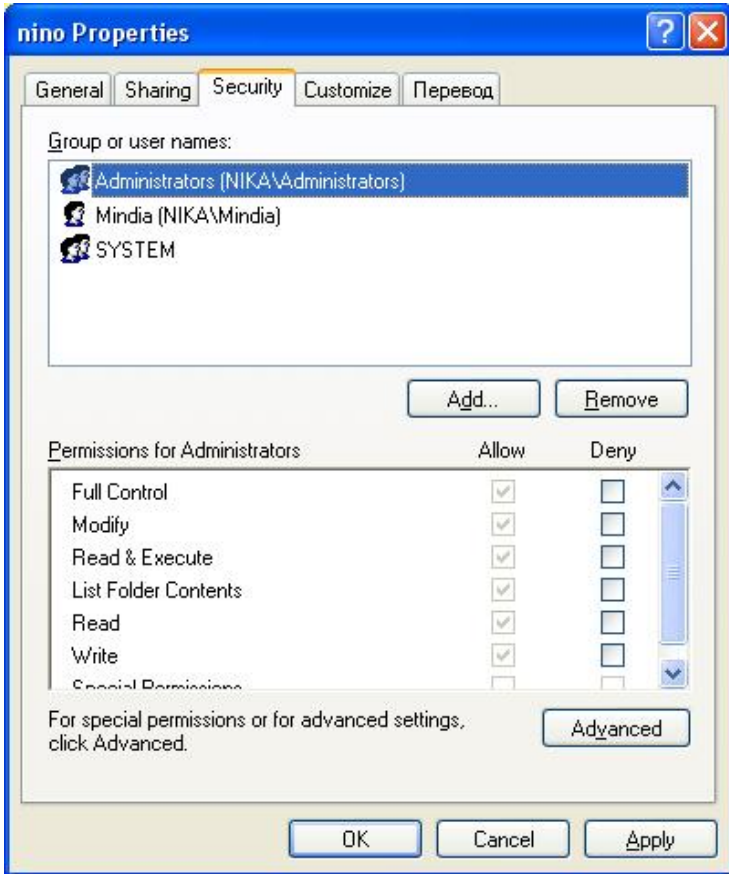
NTFS ფაილური სისტემის გამოყენებით დაფორმატებული დისკების ტომებში, მთავარი ფაილური ცხრილების (master file table) თითოეული ჩანაწერი მოიცავს მიმართვის საკონტროლო სიას ACL (access control list). ეს სია განსაზღვრავს იმ მომხმარებლებს ან ჯგუფებს, რომლებმაც აქვთ ობიექტთან მიმართვის უფლება.

ფაილის ან საქაღალდის მფლობელს უფლება აქვს მისცეს ან არ მისცეს ამ რესურსთან მიმართვის უფლება დანარჩენ მომხმარებლებს. ნახ.2.1-ზე ნაჩვენებია მიმართვის უფლებები, რომლებიც დანიშნულია ე.წ. “გაჩუმების პრინციპით”. აქ თითოეულ მომხმარებელს ფაილებსა და საქაღალდეებზე სრული კონტროლის უფლება აქვს.

როდესაც უსაფრთხოების უზრუნველყოფა მეტად მნიშვნელოვანია, სხვადასხვა მომხმარებელთა ჯგუფებს ენიჭებათ განსხვავებული მიმართვის უფლებები.

ნახაზზე მოცემულ მაგალითზე წარმოდგენილია მიმართვის უფლებათა სრული ნაკრები (საქაღალდეებისთვის C:\Winnt),

ზემოსხენებული დიალოგური ფანჯრის გასახსნელად საკვალადის კონტექსტური მენიუდან აირჩიეთ Properties→Security→ Advanced.



ნახ.2.1

ცხრილში ჩამოთვლილია მიმართვის უფლებები და მათი მოქმედების შედეგები:

მიმართვის უფლებები	მოქმედებები მომხმარებლისათვის და ჯგუფებისათვის
Full Control	ამორჩეული მომხმარებლისათვის ან ჯგუფისათვის უზრუნველყოფს სრულ

	კონტროლს ფაილებზე ან საქალაქდებზე. კერძოდ, დაათვალიეროს საქალაქდის შემცველობა, შექმნას ახალი ფაილები, წაშლოს ფაილები და ქვეკატალოგები, შეცვალოს ფაილებთან და ქვეკატალოგებთან მიმართვის უფლებები, მოიპოვოს საკუთრების უფლებები ფაილებზე.
Modify	უფლებას აძლევს ამორჩეულ მომხმარებელს ან ჯგუფს მოახდინონ ფაილების წაკითხვა, რედაქტირება, შექმნა და წაშლა, მაგრამ არ აძლევს უფლებას უფლებას შეცვალოს მიმართვის უფლებები და მიიღოს საკუთრების უფლება ფაილზე.
Read & Execute	უფლებას აძლევს ამორჩეულ მომხმარებელს ან ჯგუფს დაათვალიერონ ფაილის შემცველობა და გაუშვან პროგრამები შესრულებაზე.
List Folder Contents	ეს უფლება მოქმედებს მხოლოდ საქალაქდებისათვის. გულისხმობს იგივე უფლებებს, რასაც Read & Execute უფლება. განსხვავება იმაშია, რომ ეს მიმართვის უფლება მოქმედებს მხოლოდ საქალაქდებისათვის.
Read	უფლებას აძლევს ამორჩეულ მომხმარებელს ან ჯგუფს დაათვალიეროს ფაილების ატრიბუტები, უზრუნველყოფს ფაილების წაკითხვისა და სინქრონიზაციის შესაძლებლობას.
Write	უფლებას აძლევს ამორჩეულ მომხმარებელს ან ჯგუფს შექმნას ფაილები, ჩაწეროს მონაცემები, წაკითხოს ატრიბუტების მნიშვნელობები და მიმართვის უფლებები, ასევე შეასრულოს ფაილების სინქრონიზაცია.

2.2. პირად ღოკუმენტებთან მიმართვის ბლოკირება

Windows XP-ში შექმნილი ყოველი ახალი აღრიცხვის ჩანაწერი ავტომატურად თავსდება ჯგუფში Administrators. აქედან გამომდინარე, თუ მომხმარებლის აღრიცხვის ჩანაწერი შედის Administrators-ის ჯგუფში მას შეუძლია დაათვარიელოს ნებისმიერი მომხმარებლის საქალაღდე. შესაბამისად, ადმინისტრატორის უფლებებიდან გამომდინარე, შეუძლია შეცვალოს, წაშალოს, დაამატოს ფაილები ნებისმიერი მომხმარებლის საქალაღდეში.

მორეს მხრივ, შეზღუდული აღრიცხვის ჩანაწერის მქონე მომხმარებელს, უფლება აქვს მიმართოს მხოლოდ პირად ღოკუმენტებს My Computer საქალაღდეში. შეზღუდული უფლებების ნებისმიერი მომხმარებელი, რომელიც ეცდება სხვა მომხმარებლის პირადი ფაილების დათვალიერებას საქალაღდეში Documents and Settings, დანახავს შემდეგი სახის შეტყობინებას "Access Denied".

ამგვარად, თუ თქვენი აღრიცხვის ჩანაწერი – ესაა ერთადერთი ადმინისტრატორის აღრიცხვის ჩანაწერი კომპიუტერზე, ხოლო დანარჩენ მომხმარებლებს აქვთ შეზღუდული აღრიცხვის ჩანაწერები, ყოველგვარი რისკის გარეშე შევიძლიათ შეინახოთ პირადი ფაილები My Documents საქალაღდეში, ისე რომ არ მიანიჭოთ მას თვისება Private. თუ თქვენი კომპიუტერის აღრიცხვის ჩანაწერების ღოკალური ბაზა Administrators ჯგუფში მოიცავს ერთზე მეტ ჩანაწერს, საჭიროა ჩართოთ ოფცია Make This Folder Private.

ამასთან, მეტად საყურადღებოა ამ ოფციის შემდეგი თვისებები:

- დისკი, სადაც ინახება თქვენი პირადი პროფილი, უნდა იყოს დაფორმატებული NTFS ფაილური სისტემის საშუალებით. ეს ოფცია არ მოქმედებს, თუ დისკი დაფორმატებულია FAT32 ფაილური სისტემის გამოყენებით;

- ოფცია Make This Folder Private მისაწვდომია მხოლოდ იმ შემთხვევაში, თუ დაბლოკილია ოფცია Simple File Sharing;

- თქვენი აღრიცხვის ჩანაწერი დაცული უნდა იყოს პაროლით;

- ოფცია Make This Folder Private მისაწვდომია მხოლოდ კონკრეტული მომხმარებლის კონკრეტული პროფილისათვის. თქვენ ვერ გამოიუყენებთ ამ ოფციას იმ საქალაღდისათვის, რომელიც ეკუთვნის სხვა მომხმარებლის პროფილს.

2.3. როგორ მიმართოთ ფაილს თუ არ გვაქვს მიმართვის უფლება

თითოეულ ფაილს ან საქალაქს NTFS განყოფილებაში ჰყავს მფლობელი. მფლობელს შეუძლია მიანიჭოს ან წაართვას ფაილებთან და საქალაქებთან მიმართვის უფლება სხვა მომხმარებელსა და ჯგუფებს. როგორც მფლობელი, თქვენ შეგიძლიათ დაბლოკოთ ყველა სხვა მომხმარებელი, Administrators ჯგუფის წევრების ჩათვლით. ასევე, შეგიძლიათ გადასცეთ სხვა მომხმარებელს ამ ფაილზე ან საქალაქზე პასუხისმგებლობის უფლება. ამისათვის, შესაძლებელია შემდეგი მოქმედებები.

– თუ თქვენ ხართ ობიექტის მფლობელი

1. ფაილის ან საქალაქის კონტექსტური მენიუდან აირჩიეთ პუნქტი Properties.

2. აირჩიეთ ბრძანება Security→Advanced. გაიხსნება დიალოგური ფანჯარა Advanced Security Settings. (იხ.ნახ.2.2)

3. აირჩიეთ ოფცია Owner, ამ დიალოგურ ფანჯარაში მითითებულია მიმდინარე მფლობელის სახელწოდება. თქვენ შეგიძლიათ გადასცეთ საკუთრების უფლება ნებისმიერ მომხმარებელს ან ჯგუფს.

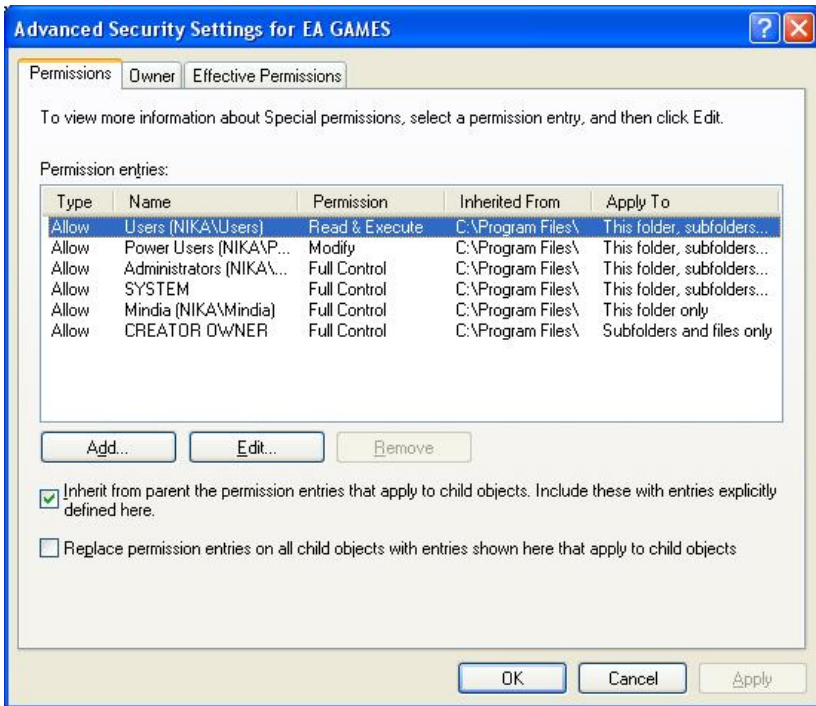
4. თუ ამორჩეული ობიექტი არის საქალაქი და თქვენ გინდათ, რომ ცვლილებები შეეხოს ამ საქალაქის ყველა ფაილსა და ქვესაქალაქს, აირჩიეთ ოფცია Replace Owner On Subcontainers And Objects.

5. აირჩიეთ სახელი სიიდან Change Owner To .

– თუ თქვენ ხართ ადმინისტრატორი, შეგიძლიათ უშუალოდ მიიღოთ საკუთრების უფლება. გახსნით დიალოგური ფანჯარა Advanced Security Settings, აირჩიეთ ოფცია Owner და სახელი სიიდან Change Owner To.

– თუ თქვენ არ ხართ ადმინისტრატორი, საჭიროა თხოვოთ მიმდინარე მფლობელს ან ადმინისტრატორს დაამატოს თქვენს აღრიცხვის ჩანაწერში ფაილს ან საქალაქის ACL და მიგანიჭოთ თქვენ Take Ownership მიმართვის უფლებები. ამისათვის, დიალოგურ ფანჯარაში Advanced Security Settings, აირჩიეთ ბრძანება Permissions →Edit.

ინფორმაციის სრული კონფიდენციალობის მისაღწევად საჭიროა დამატებითი ღონისძიებების მიღება, მაგალითად, კოდირება.



ნახ.2.2

2.4. პროგრამებთან მიმართვის ფორმირება ბრძანებათა სტრიქონიდან

მიმართვის უფლებების დათვალიერების და რელაქტირების განსხვავებული მეთოდია ბრძანებათა სტრიქონის უტილიტა Calcs.exe.

ბრძანების შესასრულებლად ბრძანებათა სტრიქონში აკრიფეთ შემდეგი ბრძანება:

calas ფაილის_სახელი

ბრძანების სინტაქსის სანახავად ბრძანებათა სტრიქონში აკრიფეთ calcs.

ეს ბრძანება მოხერხებულია იმით, რომ შეიძლება ობიექტებთან მიმართვის უფლებების სწრაფად განსაზღვრა, მრავალრიცხოვანი დილოგური ფანჯრების გარეშე.

ცხრილში განხილულია Calcs ბრძანების უტილიტები

პარამეტრი	ფუნქცია
/T	მიმართვის უფლებების შეცვლა მითითებული ფაილებისათვის მიმდინარე საქალაქდემი და ყველა მისი ქვესაქალაქდემი
/E	მიმართვის უფლებების სიის რედაქტირება
/C	დამატებით ფაილებთან მუშაობის გაგრძელება, იმ შემთხვევაშიც კი თუ მიიღეთ “Access Denied” შეტყობინება.
/G user:perm	მითითებულ მომხმარებელს მიანიჭებს მიმართვის უფლებებს; თუ გამოიყენება /E პარამეტრის გარეშე მთლიანად იცვლება მიმართვის უფლებები.
/R user	გათიშავს მიმართვის უფლებებს მითითებული მომხმარებლისათვის (უნდა გამოიყენოთ პარამეტრი /E)
/P user:perm	ცვლის მიმართვის უფლებებს მითითებული მომხმარებლისათვის
/D user	უარს ეუბნება მიმართვაზე მითითებულ მომხმარებელს

პარამეტრებისათვის /G და /P გამოიყენება ერთ-ერთი შემდეგი ოთხი სიმბოლოდან (perm-ის ნაცვლად):

- F (Full Control) – Allow ალამის ექვივალენტურია სტრიქონისათვის Full Control ჩანართში Security.
- C (Change) – Allow ალამის ექვივალენტურია სტრიქონისათვის Change ჩანართში Security.
- R (Read) – Allow ალამის ექვივალენტურია სტრიქონისათვის Read ჩანართში Security.
- W (Write) – Allow ალამის ექვივალენტურია სტრიქონისათვის Write ჩანართში Security.

2.5. პროგრამებთან მიმართვის შეზღუდვა

ნებისმიერ ადმინისტრატორს სურს შეუზღუდოს მომხმარებლებს გარკვეული პროგრამებთან მიმართვის საშუალება. ქვემოთ ჩამოთვლილია რამოდენიმე მეთოდი.

– წაშალეთ სწრაფი მიმართვის პიქტოგრამები საქალაქებიდან %AllUsersProfile%\Desktop და %All Usersprofile%\Short Menu.

– წაშალეთ ჯგუფი Everyone და მომხმარებელთა ჯგუფები მიმართვის უფლებათა სიიდან, დატოვეთ მხოლოდ ჯგუფი Administrators და Power User. (იხ. თავი. 2.1.)

– არ მისცეთ საშუალება მომხმარებლებს გაააქტიურონ პროგრამები cmd.exe და command, რომლებიც მდებარეობენ საქალაქებში com %SystemRoot%\System32. შეცვალეთ ამ ორივე ფაილთან მიმართვის წესები, ისე რომ მათი გააქტიურების უფლება ჰქონდეს მხოლოდ ადმინისტრატორს, ან გადაარქვით მათ სახელები.

– გამოიყენეთ პროგრამათა შეზღუდვის პოლოტიკები. ეს ზლიერი, თუმცა საღმადო რთული ინსტრუმენტული საშუალებები დაწვრილებითაა აღწერილი სტატიაში Microsoft Knowledge Base Q310791.

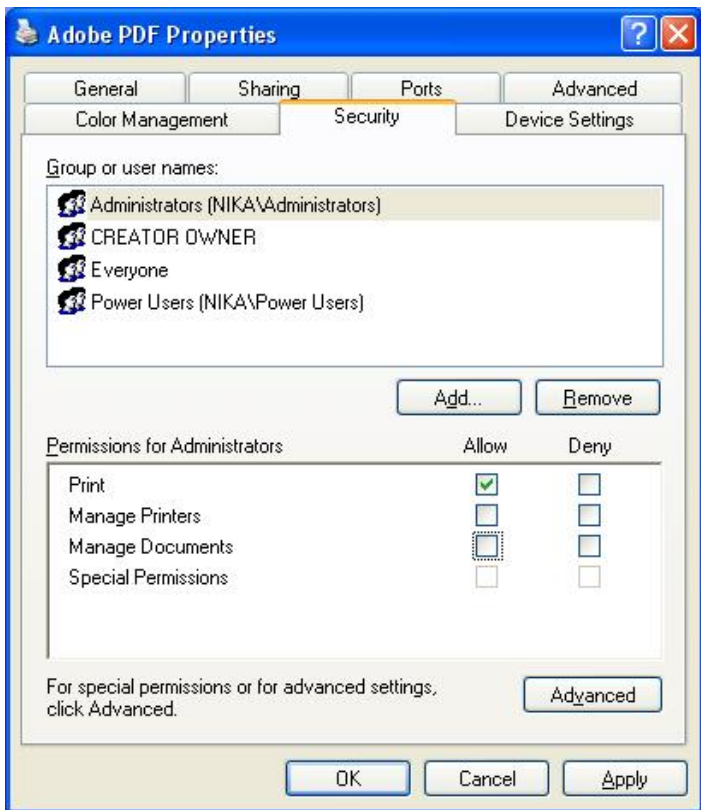
2.6. პერიფერიული მოწყობილობების მართვა

იმისათვის, რომ აკრძალოთ დისკებთან, კომპაქტ-დისკებთან, zip-დისკებთან მიმართვის საშუალება საჭიროა ფიზიკურად ჩაკეტოთ დისკები ან გამოიყენოთ Group Policy. ასევე შეგიძლიათ გამოიყენოთ უტილიტა Device Lock (<http://www.ntutility.com/dl/indec/htm>), რომელიც უზრუნველყოფს დაცვის დამატებით საშუალებებს.

ასევე შესაძლებელია აუკრძალოთ მომხმარებელს ლოკალურ პრინტერთან მიმართვის საშუალება (საჭიროა გათიშოთ ოფცია Simple File Sharing).

თითოეულ პრინტერს აქვს ოფცია Security (ნახ.3.3), სადაც ჩამოთვლილია :

- მომხმარებლები, რომლებსაც აქვთ ბეჭდვის უფლება
- მომხმარებლები, რომელთაც აქვთ დავალებების მართვის უფლება.
- მომხმარებლები, რომელთაც შეუძლიათ მართონ პრინტერის პარამეტრები.



ნახ.3.3

საკონტროლო კითხვები:

1. როგორ ჩავრთოთ Simple File Sharing ინტერფეისი და რისთვისაა იგი საჭირო?
2. შეიძლება ჩაითვალოს თვისება Private საქალაქის დაცვის საიმედო საშუალებად?
3. როგორ შევზღუდოდ ამა თუ იმ პროგრამის შესრულებაზე გაშვება?
4. რის საშუალებას იძლევა calcs ბრძანება?

თავი 3. უსაფრთხო ინტერნეტი და ელექტრონული ფოსტა

3.1. ვირუსები და მათთან ბრძოლა

კომპიუტერული ვირუსების გამოჩენა 1980 წლიდან დაიწყო, როდესაც ისინი სწრაფად ვრცელდებოდნენ ინფიცირებული დისკეტების საშუალებით. ბოლო წლებში ისინი სულ უფრო მეტად მავნე და მომხმარებლისათვის შეუმჩნეველნი გახდნენ. ინტერნეტის, ელექტრონული ფოსტის და ძალიან პოპულარული Windows-ის წყალობით ვირუსები მთელს ქვეყანაში წარმოუდგენელი სისწრაფით ვრცელდება. ექსპერტთა დაკვირვების მიხედვით, malware-ს (ყველა სახის მავნებელი პროგრამის საყოველთაოდ მიღებული დასახელება) მოცულობის ზრდა წელიწადში 15%-ს აღემატება.

მართალია, ძირითად საფრთხეს მომხმარებლებს კომპიუტერული ვირუსები უქმნიან, არსებობს სხვადასხვა სახის მავნე პროგრამებიც. განვმარტოთ მათი მუშაობის პრინციპები.

ვირუსი – ესაა პროგრამული კოდი, რომლის ტირაჟირებაც სხვა ობიექტში დამატების შედეგად ხდება. ეს პროცესი მიმდინარეობს შეუმჩნეველად, მომხმარებლის ნებართვის გარეშე, ამგვარად, ვირუსს შეუძლია ფაილების, დოკუმენტების ან ფაილური და დისკური სტრუქტურების, როგორცაა ჩასატვირთი სექტორი ან ფაილების განლაგების ცხრილი, ინფიცირება. ვირუსის გააქტიურება ხდება ინფიცირებული პროგრამის გაშვებისას. მათ შეუძლიათ მუდმივად იარსებონ მეხსიერებაში და მოახდინონ მომხმარებელთა ფაილების ინფიცირება ან საკუთარი ფაილების შექმნა, ასევე შეუძლიათ შეცვალონ მნიშვნელობები სისტემურ რეესტრში. ვირუსი, აუცილებელი არაა იყოს ცალკეული პროგრამა, და ყოველთვის არ წარმოადგენს დესტრუქციულს თავისი შინაარსით, ყველაფერი დამოკიდებულია მის ნაირსახეობაზე.

Worm (ჭია) – ესაა დამოუკიდებელი პროგრამა, რომელიც ერთი კომპიუტერიდან მეორეზე საკუთარი თავის კოპირების შედეგად ვრცელდება, როგორც წესი ლოკალური ქსელის ან საფოსტო გზავნილების საშუალებით. ეს პროგრამები ანადგურებენ მონაცემთა ფაილებს ან აწარმოებენ ერთობლივ შეტევას სხვა კომპიუტერის

წინააღმდეგ. ყოველთვის არ არსებობს მკაფიო განსხვავება ვირუსებსა და ჭიებს შორის.

ტროას ცხენები ანუ ტროიანები – პროგრამები, რომელთა გააქტიურებაც ხშირად მომხმარებლის თანხმობის შედეგად ხდება. ამ ერთი შეხედვით უწყინარ პროგრამებს შეუძლიათ შეცვალონ მომხმარებელთა პაროლები და მიმართვის უფლებები. ტროიანი შეიძლება აღმოჩნდეს კომპიუტერში საფოსტო გზავნილებიდან ან ვებ-საიტებიდან. მაგალითად, ჰაკერი რომელიმე საიტიდან ატყობინებს მსხვერპლს, რომ ინტერნეტში შეიმჩნევა ძალიან ვერაგი ვირუსის ეპიდემია და სთავაზობს მიმართოს თავის ვითომც და ანტივირუსულ პროგრამას, საიდანაც რეალურად მოხდება მისი ინფიცირება.

შერეული კოდები წარმოადგენენ ახალი კლასის დახვეწილ მავნე პროგრამებს, რომლებიც მოიცავენ ვირუსების, ჭიების და ტროიანების ყველა მახასიათებელს, რაც საშუალებას აძლევს ბოროტგანმზრახველს აწარმოოს განსაკუთრებით ეფექტური შეტევა. ასეთი პროგრამების მიზანს წარმოადგენს ვებ-სერვერები და ქსელები, რაც მნიშვნელოვნად ამაღლებს მათ საფრთხეს.

და ბოლოს, არ შეიძლება არ აღვნიშნოთ – სპამი. ყველა, ვინც სარგებლობს ელექტრონული ფოსტით, ადრე თუ გვიან დებულობს მოსაბეზრებელ სარეკლამო შეტყობინებებს ანუ სპამს. სპამი ნამდვილი უბედურებაა, რომელიც საფრთხეს უქმნის კომპიუტერის უსაფრთხოებას. იგი წარმოადგენს იდეალურ გარემოს სხადასხვა თაღლითებისათვის, რომლებიც ავრცელებენ საეჭვო მარკეტინგულ სქემებს. ამ კატეგორიის ზოგიერთი წერილი შეიცავს ვირუსებს და სხვა მავნე პროგრამებს. როგორც წესი, სპამერები ეძებენ მიაძიტ მომხმარებლებს, რომლებიც მიიღებენ შეტყობინებას და მოახდენენ მასზე რეაგირებას. ისინი მაღავენ საკუთარ მისამართებს, ამიტომაც შეუძლებელია მათი დასჯა.

არც თუ ისე მარტივი საქმეა ჩვეულებრივი წერილრბის განსხვავება სპამისაგან, თუმცა არსებობს მათთვის დამახასიათებელი თავისებურებები. კერძოდ, სპამერები იყენებენ ფიქტიურ მისამართებს (ველში From), უთითებენ უწყინარ ტექსტებს ველში Subject (მაგალითად, “თქვენ მიიღეთ ჩემი წერილი?” ან “ინფორმაცია, რომელიც თქვენ შეუკვეთეთ”), ცდილობენ ჩართონ წერილში მიმართვა “ერთჯერად” ვებ-გვერდებზე, რომელიც ქრება მას შემდეგ, როდესაც ვინმე წამოეგება ანკესზე.

დაწვრილებით სპამერების ტექნოლოგიები აღწერილია ვებ-საიტზე <http://www.spamfaq.net/spamfighting.shtml>.

გთავაზობთ ზოგიერთი ანტივირუსული პროგრამის მოკლე დახასიათებას.

Aladdin Knowledge Systems

პროდუქტები: eSafe Desktop, eSafe Enterprises

ეს პაკეტი აერთიანებს ანტივირუსულ ტექნოლოგიებს, პერსონალურ ბრანდმაუერს, საფოსტო ფილტრს და სამუშაო მაგიდის ბლოკირების უტილიტებს. შესაძლებელია 60-დღიანი დემო-ვერსიის გადმოტვირთვა ვებ-საიტიდან: <http://www.aks.com>.

ინფორმაცია ვირუსების შესახებ:

<http://www.aks.com/home/csrt/valerts.asp>

Central Command

პროდუქტები: Vexira Antivirus (ვერსიები: Home, Small Business, Enterprise, Government, Educational Edition).

ესაა გამოსაყენებლად მარტივი სკანერები, რომელთა საშუალებითაც შეგიძლიათ შეამოწმოთ ელექტრონული ფოსტა, ჩასატვირთი ფაილები და ქსელური დისკები. თითოეული პროდუქტისათვის არსებობს დემო-ვერსია.

ვებ-საიტი: <http://www.centralcommand.com>

ინფორმაცია ვირუსების შესახებ:

http://www.centralcommand.com/recent_threats.html

Command Software Systems, Inc.

პროდუქტები: Command AntiVirus, სახლის და კორპორატიული ვერსია.

ეს პროგრამა ამოწმებს 70 ტიპის (მათ შორის შეკუმშულ) ფაილებს, აუცილებლობის შემთხვევაში ვებ-გვერდებსაც. ხელმისაწვდომია 30-დღიანი დემო-ვერსია ვებ-საიტზე: <http://www.commandcom.com>

ინფორმაცია ვირუსების შესახებ:

<http://www.commandcom.com/virus/index.cfm>

Computer Associates International, Inc.

პროდუქტები: eTrust EZ Armor, eTrust EZ Antivirus, eTrust EZ Deskshield, eTrust EZ Firewall.

კომპანია CAI გვთავაზობს პროდუქტების ფართო სპექტრს, როგორც სახლის, ისე მცირე ბიზნესისა და მსხვილი კორპორაციებისათვის.

ვებ-საიტი: <http://www.cai.com>, <http://www2.my-etrust.com>.

ინფორმაცია ვირუსების შესახებ:

<http://www3.ca.com/virus>

ESET

პროდუქტი: NOD32

პრეგრაამს უზრუნველყოფს კომპიუტერის მუდმივ დაცვას, შეუძლია ინტეგრირება Windows Explorer-თან და საფოსტო კლიენტებთან. პაკეტი შეიცავს განახლების მრავალ ვარიანტს, რომელშიც გათვალისწინებულია ლოკალურ ქსელში მუშაობის თავისებურებები.

ვებ-საიტი: <http://www.nod32.com>

ინფორმაცია ვირუსების შესახებ:

<http://www.nod32.com/aupport/pedia.htm>

F-Secure Corp.

პროდუქტი: F-Secure Anti-Virus

კომპანის გვთავაზობს თავისი პროგრამის ათზე მეტ ვერსიას. მათ რიცხვში შედის პერსონალური და კორპორატიული პროგრამების ათზე მეტი ვერსია. პაკეტი Total Suite მოიცავს ბრანდმაუერისა და ანტივირუსის ფუნქციებს. ხელმისაწვდომია სადემონსტრაციო ვერსიები:

ვებ-საიტი: <http://www.f-secure.com>

ინფორმაცია ვირუსების შესახებ:

<http://www.f-secure.com/virus-info>

Grisoft, Inc.

პროდუქტები: AVG Antivirus 6.0 (უფასოდ ვრცელდება ვერსიები Professional და Server)

კომპლექტში შედის ანტივირუსული სკანერი და ელექტრონული ფოსტის დაცვის სისტემა ავტომატური განახლების ფუნქციებით. ხელმისაწვდომია 30-დღიანო დემო-ვერსია.

ვებ-საიტი: <http://www.grisoft.com>

ინფორმაცია ვირუსების შესახებ:

http://www.grisoft.com/html/us_alert.php

კასპერსკის ლაბორატორია

პროდუქტი: კასპერსკის ანტივირუსი.

პროგრამას შეუძლია ინტეგრირება Outlook Express-თან და MS Office-ის პროდუქტებთან.

ვებ-საიტი: <http://www.kasperskylabs.com>

ინფორმაცია ვირუსების შესახებ:

<http://www.kasperskylabs.com/news.html?news=20140>

Network Associates(McAfee)

პროდუქტები: McAfee VirusScan, McAfee Clinic, McAfee NetShield, McAfee WebShield, McAfee GroupShield.

სოლიდური ფირმა, გეთავაზობს ანტივირუსული პროგრამების ფართო არჩევანს სახლში მომუშავე მომხმარებლებისათვის, კერძო მეწარმეებისათვის და მსხვილი კორპორაციებისათვის. თითოეული პროდუქტისათვის ხელმისაწვდომია სადემონსტრაციო ვერსია.

ვებ-საიტი: <http://www.nai.com>, <http://www.mcafee.com>,
<http://www.mcafee2b.com>.

ინფორმაცია ვირუსების შესახებ:

<http://vil.nai.com/VIL/default.asp>

Norman ASA

Virus Control, Norman Personal Firewall, Norman Privacy.

პროგრამული პაკეტი შედგება მოღულებსაგან, რომელიც შეიცავს რეზიდენტულ სკანერს, სკანერს ხელით შემოწმებისათვის, განახლების სისტემას და უტილიტების ნაკრებს. ადმინისტრატორს შეუძლია ააწყოს სისტემა ისეთი სახით, რომ კლიენტების პროგრამების განახლება მოხდეს ინტერნეტიდან. საიტზე მოთავსებულია 30-დღიანი დემო-ვერსია.

ვებ-საიტი: <http://www.norman.com>

ინფორმაცია ვირუსების შესახებ:

http://www.norman.com/virus_info/virus_descriptions.shtml

Panda Software

პროდუქტი: Panda Antivirus

შემოთავაზებული პროგრამული კომპლექსი უზრუნველყოფს ლოკალური ქსელის (სერვერის და კლიენტ-კომპიუტერების) სრულ დაცვას. სახლში მომუშავე მომხმარებლებს შეუძლიათ შეიძინონ Titanium ან Platinum ვერსია, რომელთა განახლებაც ხდება ყოველდღე და თავსებადია WindowsXP-სთან.

ვებ-საიტი: <http://www.pandasoftware.com>,

ინფორმაცია ვირუსების შესახებ: <http://www.pandasoftware.com>

Sophos

პროდუქტი: Sophos Anti-Virus

პროგრამა დამუშავებულია სპეციალურად კორპორატიული ქსელებისათვის, ახორციელებს დისკების, შესრულებადი ფაილების, დოკუმენტების და ქსელური დისკების მონიტორინგს. ხელმისაწვდომია სასინჯი ვერსია

ვებ-საიტი: <http://www.sophos.com>,

ინფორმაცია ვირუსების შესახებ: <http://www.sophos.com/virusinfo>

Symantec Corp.

პროდუქტები: Norton Antivirus, Norton Internet Security

პროდუქტები განკუთვნილია, როგორც ცალკეულ მომხმარებლებისათვის, ისე ნებისმიერი ზომის ფირმებისათვის. Norton Internet Security-ის შემადგენლობაში შედის ბრანდმაუერი, ხოლო Norton Antivirus-ი კარგად ინტეგრირდება საფოსტო პროგრამებთან და მუშაობს ლოკალურ ქსელში.

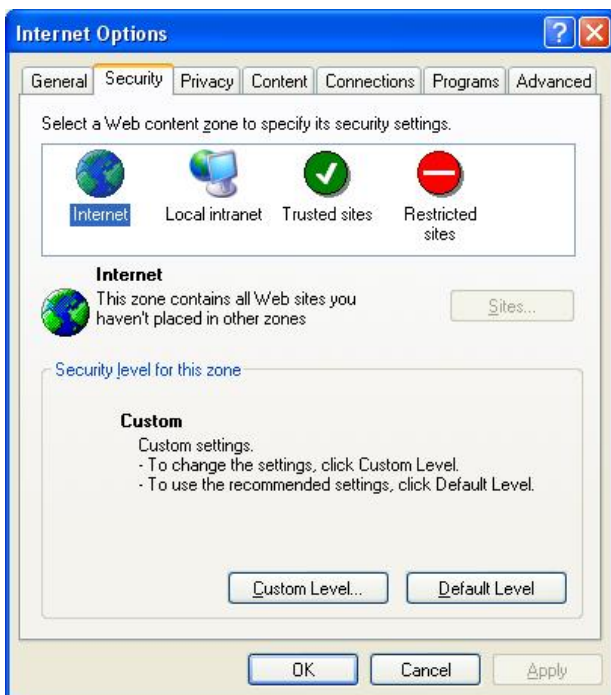
ვებ-საიტი: <http://www.symantec.com>,

ინფორმაცია ვირუსების შესახებ: <http://www.sarc.com>

3.2. უსაფრთხოების ზონები

უსაფრთხოების ზონები წარმოადგენს ინტერნეტის მომხმარებელთა თავდაცვის ძირითად საშუალებას. გაჩუმების პრინციპით ყველა ვებ-საიტი მიეკუთვნება ინტერნეტის ზონას, ხოლო Internet Explorer-ი მკაცრად განსაზღვრავს მოქმედებათა სახეებს ამა თუ იმ ზონის ვებ-საიტებისათვის. კერძოდ, არსებობს უსაფრთხოების ოთხი ზონა:

- ლოკალური ინტრაქსელი (Local Intranet). ეს ზონა განკუთვნილია ვებ-საიტების განსათავსებლად ორგანიზაციის შიგნით;
- სანდო ვებ-საიტები (Trusted Sites). ამ საიტებს ენიჭებათ ნდობის უმაღლესი დონე. (მაგალითად, ვებ-საიტები თქვენი საქმიანი პარტნიორებისათვის);



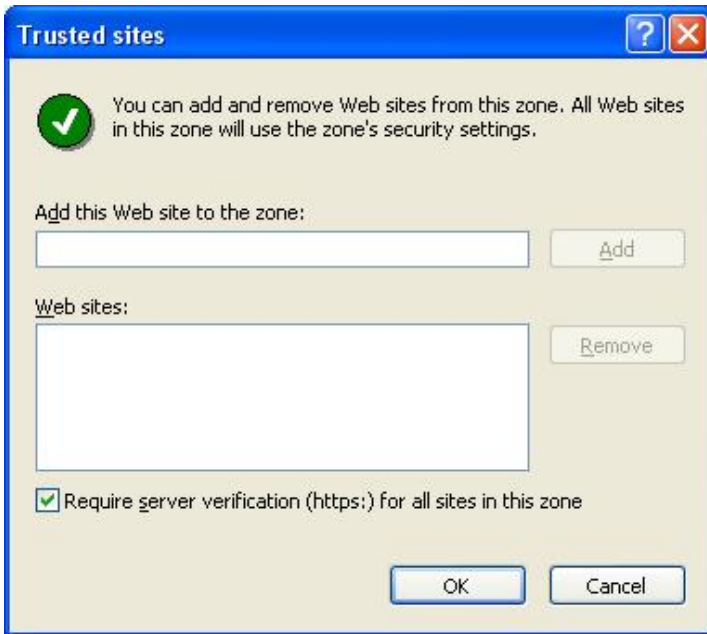
ნახ.3.1

- შეზღუდული ვებ-საიტები (Restricted Sites zone). ესაა საიტები, რომლებსაც დანამდვილებით არ ენდობით.

- ინტერნეტი (Internet Zone). ეს ზონა განკუთვნილია იმ ვებ-საიტებისათვის, რომლებიც არ მოხვდნენ არც ერთ წინა კატეგორიაში.

უსაფრთხოების ზონების კონფიგურირებისათვის შეასრულეთ შემდეგი ბრძანებები: Tools→Internet Options→Security. იხ.ნახ.3.1.

ვებ-საიტის ზონაში ჩასამატებლად აირჩიეთ ზემოჩამოთვლილი ზონიდან ერთ-ერთი და ველში Add this Web site to the zone , აკრიფეთ ვებ-საიტის URL-ლინკი და დააჭირეთ ღილაკს OK. იხ.ნახ.3.2.



ნახ.3.2

ოვცია Require server verification (https:) for all sites in this zone (ამ ზონის ყველა კვანძისათვის აუცილებელია (https:) სერვერების შემოწმება. თუ საჭიროა ისეთი ვებ-საიტის ჩამატება, რომელიც არ იყენებს HTTPS პროტოკოლს, საკმარისია ალამის გამორთვა.

3.3. ციფრული სერთიფიკატები

ციფრული სერთიფიკატები Ms Windows-ის უსაფრთხოების სტრუქტურის მნიშვნელოვან კომპონენტს წარმოადგენს. სერთიფიკატი – ესაა ჩანაწერი, რომელიც გამოიყენება აუტენტიფიკაციის, კოდირების ან ორივე ამ მოქმედების ერთდროულად შესრულების მიზნით.

აუტენტიფიკაცია – ესაა პროცედურა, რომლის საშუალებითაც დასტურდება პიროვნების, ორგანიზაციის ან ტექნიკური მოწყობილობის ნამდვილობა. მაგალითად, თუ თქვენ ღებულობთ ელექტრონულ შეტყობინებას ციფრული ხელმოწერით, ეს იმის გარანტიაა, რომ პიროვნება აღნიშნული, როგორც „გამომგზავნი“, სწორედ ეს პიროვნებაა და არა სხვა.

კოდირების საშუალებით შესაძლებელია ინფორმაცია დაუმალოთ ისეთ მომხმარებლებს, რომელთაც არ აქვთ მასთან მიმართვის უფლება. ამ პროცესში გამოიყენება გასაღებები, რომლებიც ახდენენ მონაცემების გადაყვანას საბაზო ფორმატიდან ისეთ ფორმატში, რომელსაც ვერ აღიქვავს მომხმარებელი. იმისათვის, რომ შესაძლებელი გახდეს ამ მონაცემების კვლავ აღქმა, არსებობს მხოლოდ ერთი გზა – უკუგარდაქმნა. (ამ დროს ისევ საჭიროა გასაღები).

მონაცემთა კოდირების ყველაზე უფრო ეფექტური და ძველი მეთოდია – სიმეტრიული კოდირება. ამ დროს მონაცემთა კოდირებისა და დეკოდირებისათვის გამოიყენება ერთი გასაღები. არასიმეტრიული კოდირება იყენებს განსხვავებულ გასაღებებს მონაცემთა კოდირება/დეკოდირებისათვის.

დღეს, ყველაზე მეტად გავრცელებულია სიმეტრიული კოდირების ერთ-ერთი მეთოდი – კოდირება საერთო გასაღებით. ამ დროს არსებობს დახურული გასაღები, რომელთანაც მიმართვის უფლება აქვს მხოლოდ ერთ სუბიექტს და ღია გასაღები, რომელთანაც მიმართვის უფლება აქვთ ყველა დანარჩენ მომხმარებლებს. მონაცემები, კოდირებული ღია გასაღებით, შეიძლება დეკოდირებული იყოს მხოლოდ შესაბამისი დახურული გასაღებით.

მაგალითად, თქვენ უგზავნით კერძო შეტყობინებას ანას. თუ გამოიყენებთ მის ღია გასაღებს შეტყობინების კოდირებისათვის, მაშინ დეკოდირების ოპერაცია შეუძლია ჩაატაროს მხოლოდ ანამ, რადგან მას

აქვს დახურული გასაღები. როგორ მივიღოთ ანას დახურული გასაღები? რა თქმა უნდა, მან ის უნდა გამოგიგზავნოთ. მაგრამ როგორ დავრწმუნდეთ რომ ის ნამდვილად ანამ გამოგზავნა? ამაში დაგვეხმარება სერტიფიკატის მნიშვნელოვანი თვისება: აუტენტიფიკაცია. შეტყობინება, ანამ გამოგზავნა თავისი გასაღები, ხელმოწერილია მესამე პირის (რომელსაც ენდობით თქვენც და ანაც) მიერ. ვინაიდან ენდობით აღჭურვილი პირი ერთადერთია, რომელსაც შეუძლია ხელი მოაწეროს შეტყობინებას თავისი დახურული გასაღებით, თქვენ რწმუნდებით, რომ შეტყობინება ნამდვილად ანას გამოგზავნილია.

ციფრული სერთიფიკატები უზრუნველყოფენ ღია გასაღების შენახვისა და გაგზავნის მექანიზმს. ადამიანს, ორგანიზაციას ან კომპიუტერს, რომელსაც მიეცემა სერთიფიკატი, შეუძლია გაავრცელოს ღია გასაღები სერტიფიკატის გადაგზავნის საშუალებით. სერთიფიკატი შეიცავს შემდეგი სახის ინფორმაციას

- სუბიექტის ღია გასაღები;
- სუბიექტის პირად მონაცემებს, როგორიცაა სახელი ან ელექტრონული მისამართი;
- სერთიფიკატის მოქმედების ვადა;
- იმ სერთიფიკაციის ცენტრის CA (Certification authority) დასახელებას, რომელმაც გასცა სერთიფიკატი;
- სერთიფიკაციის ცენტრის ციფრული ხელმოწერას, რომელმაც გასცა სერთიფიკატი.

სერთიფიკაციის ცენტრები

CA-ს დანიშნულებაა იმ ღია გასაღებების აუტენტიფიკაცია, რომლებიც ეკუთვნის მომხმარებლებს ან სხვა სერთიფიკაციის ცენტრებს. ამ ფუნქციების განსახორციელებლად CA გასცემს სერთიფიკატებს, რომელიც ხელმოწერილია მათი საკუთრი დახურული გასაღებით, ახორციელებს სერთიფიკატის სერიულ ნომერთან დაკავშირებულ ოპერაციებს და აუცილებლობის შემთხვევაში გააუქმებს სერთიფიკატს.

იმისათვის, რომ სერთიფიკატი განსახვრული იყოს, როგორც მოქმედი, ელექტრონული ტრანზაქციის ორივე მხარე უნდა ენდობოდეს სერთიფიკაციის ცენტრს (CA). თქვენს კომპიუტერზე „გაჩურების პრინციპით“ მოთავსებულია მრავალი სერთიფიკატი, რომლებიც გაცემულია სანდო CA-ს მიერ. ისინი მოთავსებულია საცავში Trusted

Root Certification Authorities. ეს სერთიფიკატი აქტიურდებიან ციფრული ხელმოწერის მქონე პროგრამის ჩატვირთვის შემთხვევაში. ამ დროს სერთიფიკატები გამოიყენება ავტომატურად, თქვენგან დამოუკიდებლად. სერთიფიკატები გამოიყენება იმ შემთხვევაშიც, თუ მომხმარებელი მიმართვს დაცულ ვებ-საიტს (Internet Explorer-ის ფანჯარაში სტატუსის პანელზე გამოსახულია ბოქლომი) კოდირებული მიერთების განსახორციელებლად.

ნახაზ3.3.-ზე გამოსახულია სერთიფიკატი, რომლის მიმართაც არ არის დადასტურებული სანდო დამოკიდებულება, რადგან ის არ არის გაცემული ძირითადი სანდო CA-ს მიერ.



ნახ.3.3

თუ გსურთ დაიცვათ თქვენი წერილები არასანქცირებული მიმართვისაგან ან გამოაქვეყნოთ ინტერნეტში რომელიმე პროგრამული პროდუქტი, საჭიროა იქონიოთ სერთიფიკატები. სერთიფიკატის შექმნა შეიძლება სერთიფიკაციის ცენტრებში. ცენტრების უმრავლესობა აწესებს გარკვეულ ფასებს სერთიფიკატებზე და თითოეული მათგანი

იყენებს პიროვნების დადასტურების სხვადასხვა ხერხებს. ვებ-საიტზე <http://office.microsoft.com/assistance/2000/cerpage.aspx>. ფირმა Microsoft-ი აქვეყნებს სერთიფიკაციის ცენტრების სიას. ფირმა Thawte-ი (<http://www.thawte.com>) გარკვეული რეგისტრაციის გავლის შემდეგ, სერთიფიკატებს გასცემს უფასოდ. ნახ.3.4.-ზე ნაჩვენებია Thawte-ის მიერ გაცემული სერთიფიკატი.



ნახ.3.4

ციფრული სერთიფიკატების თვისებები

ციფრული სერთიფიკატების თვისებების დასათვალისწინებლად შეასრულეთ შემდეგი მოქმედებები:

1. გააქტიურეთ Internet Explorer-ი;
2. აირჩიეთ ბრძანება Tools → Internet Options → Content → Certificates;

3. აირჩიეთ სერთიფიკატი – ორჯერ დააჭირეთ თავუს მარცხენა ღილაკს მის დასახელებაზე იხილეთ ნახ. 3.5. ეკრანზე გამოჩნდება დიალოგური ფანჯარა, რომელიც შედგება შემდეგი ჩანართებისაგან.



ნახ3.5

– General, აღწერილია სერთიფიკატის დანიშნულება. ცხრილში ჩამოთვლილია სერთიფიკატების გამოყენების ზოგადი სფეროები:

ცხრილი

გამოყენების სფერო	აღწერა		
კლიენტის აუტენტიფიკაცია	გამოიყენება სერვერებთან აუტენტიფიკაციისათვის	კლიენტების საკუთარი	მიერ თავის
სერვერის აუტენტიფიკაცია	გამოიყენება კლიენტებთან აუტენტიფიკაციისათვის	სერვერების საკუთარი	მიერ თავის

პროგრამული კოდის ხელმოწერა	გამოიყენება პროგრამული კოდის მწარმოებლების მიერ პროგრამების აუტენტიფიკაციისათვის
ელექტრონული შეტყობინებების დაცვა	გამოიყენება ელექტრონული შეტყობინებების ხელმოწერისა და კოდირებისათვის პროტოკოლით Secure/Multipurpose Internet Mail Extensions (S/MIME)
ნდობის სიების ხელმოწერა	გამოიყენება სერთიფიკატების ნდობის სიის შესაქმნელად
კოდირებული ფაილური სისტემა	გამოიყენება სიმეტრიულ გასაღებთან ფაილების კოდირება/დეკოდირებისათვის
ფაილების აღდგენა	გამოიყენება სიმეტრიულ გასაღებთან ფაილების აღდგენისათვის

- Details, ჩამოთვლილია სერთიფიკატის ყველა პარამეტრი და მითითებულია მისი მოქმედების ვადა;
- Certification Path, ასახულია აუტენტიფიკაციის სრული ჯაჭვი.

სერთიფიკატების მართვა

სერთიფიკატების მართვა შეიძლება ორი გზით: დიალოგური ფანჯრიდან Certificates და Microsoft-ის მართვის კონსოლიდან Certificates.

დიალოგური ფანჯრა Certificates

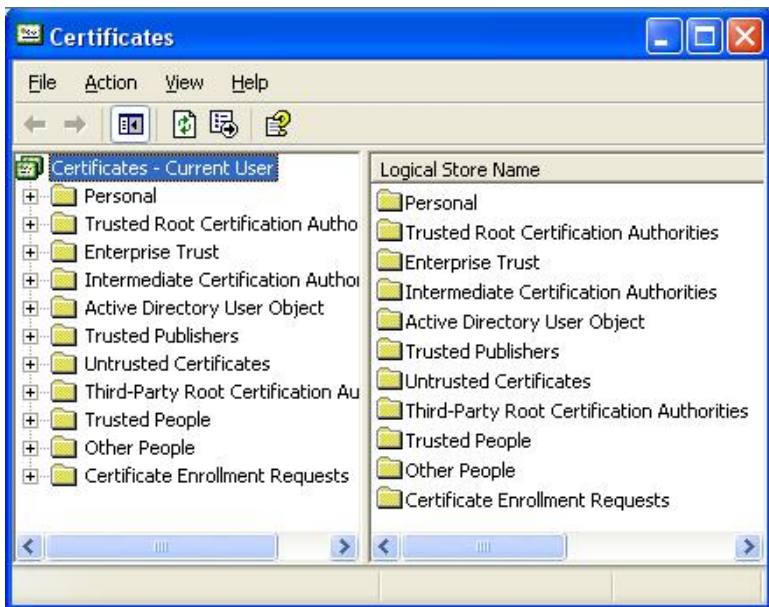
დიალოგური ფანჯრა Certificates-ის ეკრანზე გამოსატანად შეასრულეთ შემდეგი მოქმედებები:

1. გააქტიურეთ Internet Explorer-ი;
2. აირჩიეთ ბრძანება Tools → Internet Options → Content → Certificates;
3. ეკრანზე გამოჩნდება ნახ.3.6-ზე ნაჩვენები დიალოგური ფანჯრა მოცემულ დიალოგურ ფანჯარაში წარმოდგენილია სერთიფიკატების საცავი, სადაც სერთიფიკატები დაჯგუფებულია დანიშნულების მიხედვით.

- Personal (პირადი) აქ ინახება სერთიფიკატები შესაბამის დახურულ გასაღებთან ერთად (როგორც წესი, პირადი სერთიფიკატები).

- Other People (სხვა მომხმარებლები). აქ ინახება სერთიფიკატები იმ მომხმარებლებისათვის, რომლებთან ერთადაც თქვენ იყენებთ ერთ ან რამოდენიმე კოდირებულ ფაილს.

- Intermediate Certification Authorities (სერთიფიკაციის შუალედური ცენტრები). აქ ინახება სერთიფიკატები გაცემული ისეთი ცენტრების მიერ, რომლებიც არ მიეკუთვნებიან ძირითად სანდო სერთიფიკაციის ცენტრებს.



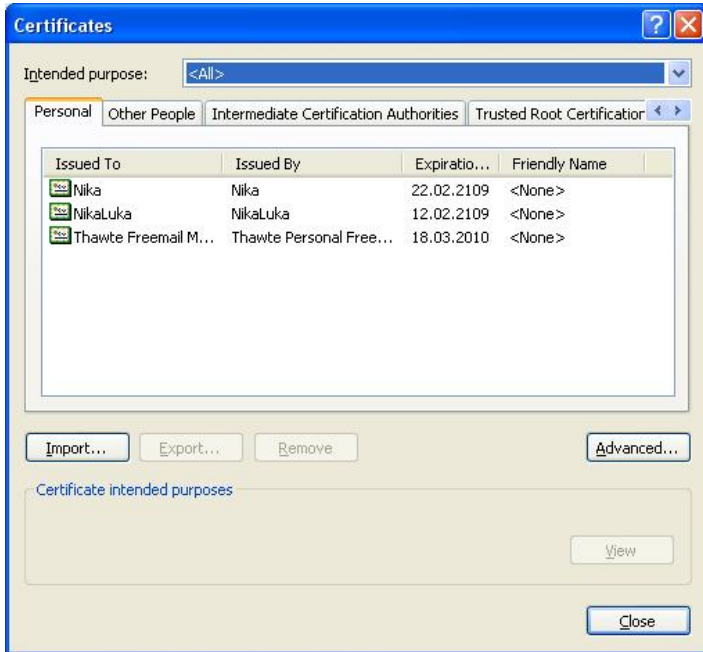
ნახ.3.6

- Trusted Root Certificates (სერთიფიკაციის სანდო მთავარი ცენტრები). აქ შენახულია ხელმოწერილი სერთიფიკატები. თქვენ შეგიძლიათ სრულად ენდოთ ცალკეული პირებისაგან ან ფირმებიდან მიღებულ ინფორმაციას, თუ თანმხლები სერთიფიკატები გაცემულია ამ კატეგორიაში მითითებული სერთიფიკაციის ცენტრების მიერ.

- Trusted Publishers (სანდო გამომცემლები). აქ მოთავსებულია მხოლოდ ის სერთიფიკატები, რომლებსთვისაც დაყენებული იყო

ალაბი Always trust Content From (ყოველთვის ენდეთ შინაარსს) დიალოგურ ფანჯარაში Security Warning.

სერთიფიკატების მართვისათვის მეტად ხელსაყრელია – კონსოლი certmgr.msc. აკრიფეთ ეს ბრძანება ბრძანებათა სტრიქონში. ეკრანზე გამოჩნდება ნახ.3.7-ზე ნაჩვენები ფანჯარა.



ნახ.3.7

სერთიფიკატების ექსპორტი და იმპორტი

შესაძლებელია სერთიფიკატების ექსპორტი სერთიფიკატების საცავიდან ჩვეულებრივ ფაილში, რაც შეიძლება დაგჭირდეთ შემდეგი მიზნის მისაღწევად:

- სარეზერვო ასლის შესაქმნელად;
- სერთიფიკატის კოპირებისათვის ან მის გადასატანად სხვა კომპიუტერზე.

ექსპორტის განსახორციელებლად Certificates დიალოგურ ფანჯარაში ამოირჩიეთ სერთიფიკატი და დაჭირეთ ღილაკს Export.

ეკრანზე გამოჩნდება Certificate Export Wizard ოსტატი. იხილეთ ნახ.3.7.

სერთიფიკატის იმპორტი აუცილებელია შემდეგი ამოცანების მისაღწევად:

- ახალი სერთიფიკატის ინსტალაციისას (სერთიფიკატი შეიძლება მიიღოს სხვა ადამიანის ან სერთიფიკატის ცენტრიდან);
- დაზიანებული ან დაკარგული სერთიფიკატის აღსადგენად;
- თქვენი პერსონალური სერთიფიკატის სხვა კომპიუტერზე დასაყენებლად.

იმპორტის განსახორციელებლად Certificates დიალოგურ ფანჯარიში დააჭირეთ ღილაკს Import

3.4. ელექტრონული ფოსტის დაცვა S/MIME-ის საშუალებით

მრავალი პოპულარული საფოსტო კლიენტური პროგრამა (Outlook, Outlook Express და Netscape Messenger), უზრუნველყოფს შეტყობინებების დაშიფრვასა და ხელმოწერას სტანდარტული უსაფრთხო ფორმატის მხადაჭერით. ესაა Secure/Multipurpose Internet Mail Extensions (S/MIME). მისი საშუალებით ინფორმაციის დაშიფრვა შესაძლებელია ციფრული სერთიფიკატის მიღების შემდეგ.

იმისათვის, რომ გაგზავნოთ დაშიფრული შეტყობინება, აუცილებელია გქონდეთ ადრესატის ღია გასაღები, რომელიც ციფრული სერთიფიკატის შემადგენელ კომპონენტს წარმოადგენს. (იხ.3.8). ღია გასაღების გასაგზავნად საკმარისია გაუგზავნოთ ადრესატს დაშიფრული შეტყობინება. მხოლოდ ის ადრესატები შეძლებენ დაშიფრული შეტყობინების მიღებას, რომლებსაც უკვე აქვთ მიღებული ციფრული სერთიფიკატი.

მას შემდეგ, რაც მიიღებთ ღია გასაღებს თქვენი კორესპონდენტისაგან, შეძლებთ დაშიფრული შეტყობინების გაგზავნას.

Microsoft Outlook-ის შემთხვევაში შეასრულეთ შემდეგი ბრძანებები:

1. მოამზადეთ შეტყობინება ჩვეულებრივი წესით;
2. აირჩიეთ Office Button→Properties→Security.

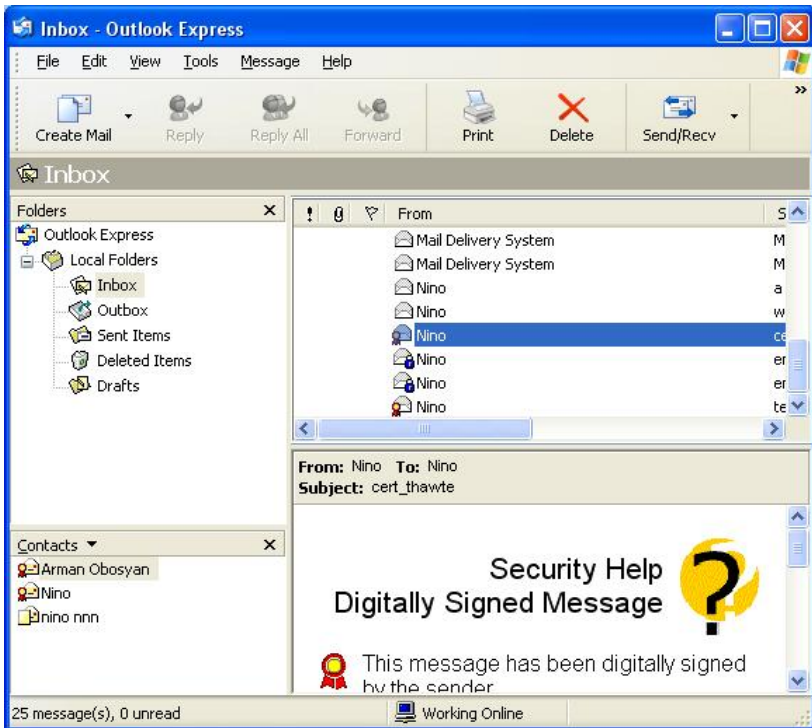
ჩართეთ ალაში Encrypt message contents and attachments, ხოლო ციფრული ხელმოწერისათვის აირჩიეთ ალაში Add digital signature do outgoing messages.

ყველა შეტყობინების დაშიფრვისათვის აირჩიეთ ბრძანება:

Tools→ Options→Trust Center→E-Mail Security და ჩართეთ ალაბი Encrypt Contents And Attachments For Outgoing Messages.

Outlook Express-ის შემთხვევაში შეასრულეთ შემდეგი ბრძანებები:

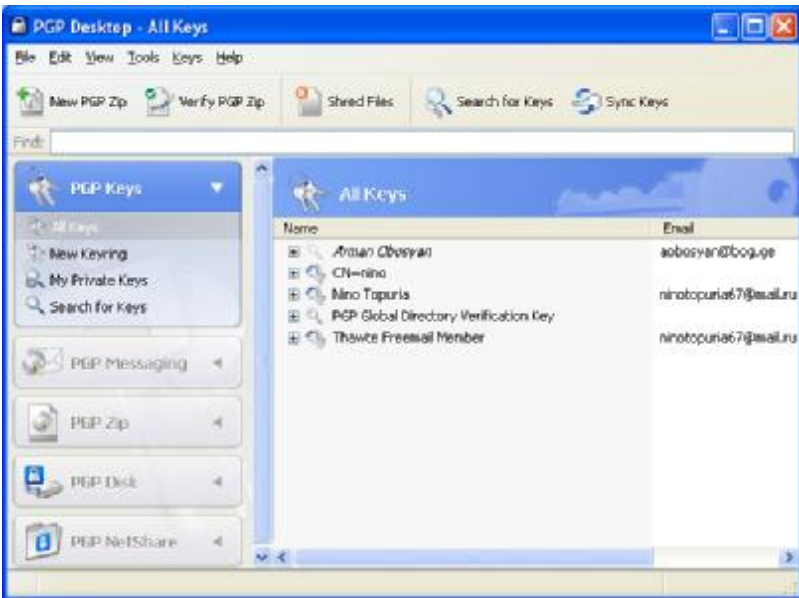
1. შექმნით შეტყობინება ჩვეულებრივი წესით;
2. აირჩიეთ Tools→Encrypt.
3. ციფრული ხელმოწერისათვის აირჩიეთ ბრძანება Tools→Digitally Sign.
4. დაშიფრულ შეტყობინებაზე გამოსახულია ბოქლომი, ხოლო ციფრული ხელმოწერა აღნიშნულია სპეციალური სიმბოლოთი – შტამპით. იხილეთ ნახ.3.8.



ნახ.3.8

3.5. ინფორმაციის დამიფრვა PGP-ის საშუალებით

წინა თავში განხილული S/MIME პროცედურების ალტერნატივას წარმოადგენს პროტოკოლი Pretty Good Privacy (PGP). ეს პროტოკოლი დღესდღეობით პრაქტიკულად წარმოადგენს ქსელში შიფრაციის სტანდარტს. ზოგიერთი მას “ოქროს” სტანდარტად მიიჩნევს. იგი შექმნა ფილ ციმერმანმა 1991 წელს. PGP-ი საშუალებას იძლევა საიმედოდ დაიცვათ დისკებზე არსებული ფაილები და საკუთარი ელექტრონული ფოსტა უცხო პირებისაგან. ყოველგვარი საშიშროების გარეშე გადასცეთ და მიიღოთ მნიშვნელოვანი ინფორმაცია. პროგრამა აგებულია ღია გასაღებით დამიფრვის პრინციპზე, რისთვისაც საჭიროა გასაღებების გენერაცია. ეს პროცესი შემდეგში მდგომარეობს: თავდაპირველად საჭიროა ღია გასაღების გენერაცია და მისი გაგზავნა ღია გასაღებების სერვერზე (ან კონკრეტული ადრესატისათვის), საიდანაც მის მიღებას შეძლებს ნებისმიერი მსურველი. ამ გასაღებით მოხდება ინფორმაციის დამიფრვა თქვენთვის, ხოლო თქვენ მიიღებთ რა ადრესატის ასევე ღია გასაღებს, შეძლებთ დამიფროთ ინფორმაციის მისთვის.



ნახ.3.9

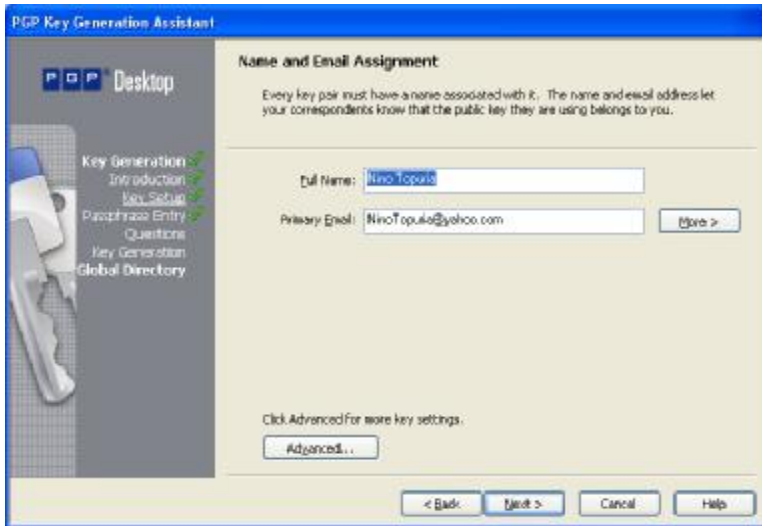
PGP-ის გააქტიურებისას ეკრანზე გამოჩნდება ფანჯარა იხილეთ ნახ.3.9, სადაც ერთი გასაღები ნიშნავს ღია გასაღებს, რომელიც მიღებულია ფოსტით ან რაიმე სხვა საშუალებით, ხოლო გასაღებების აცმა ესაა, გასაღებების წყვილი: ღია გასაღები (Public Key) და დახურული გასაღები (Private Key).

გასაღების გენერაცია

ახალი გასაღების გენერაციისათვის აირჩიეთ ბრძანება File→ New PGP Key .

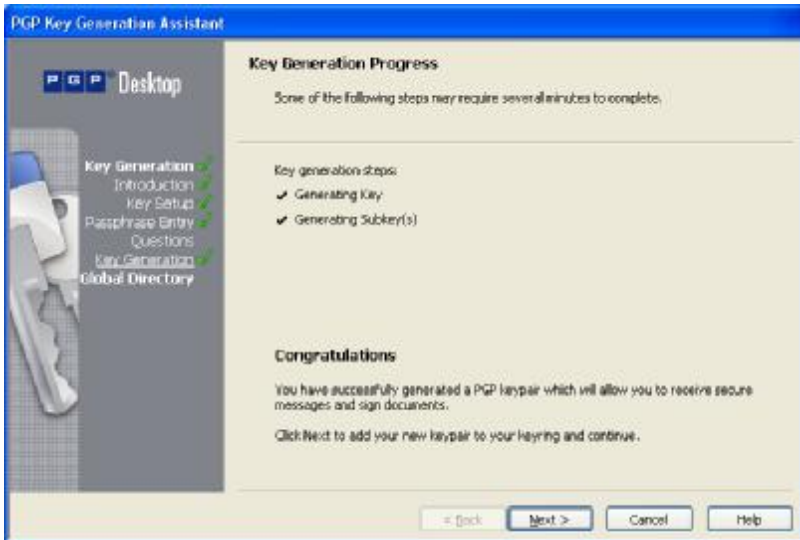
ეკრანზე გაიშვება ოსტატი, რომლის კარნახებიც ზუსტად უნდა შეასრულოთ.

- პირველ ბიჯზემორე ბიჯზე მხოლოდ დააჭირეთ კლავშს Next;
- მეორე ბიჯზე აკრიფეთ სახელი და ე-მეილი. დამატებითი პარამეტრების მისათითებლად აირჩიეთ ღილაკი Advanced. იხილეთ ნახ. 3.10.



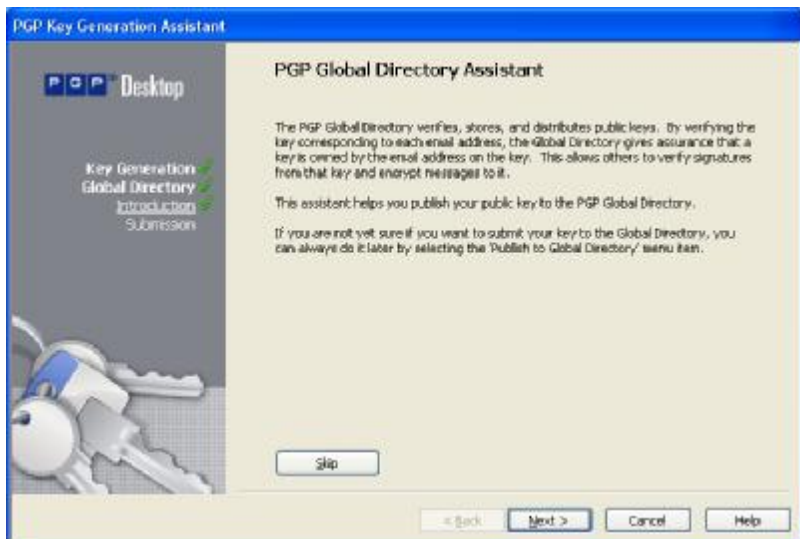
ნახ.3.10

მესამე ბიჯზე აკრიფეთ პაროლი, რომლითაც იქნება დაცული თქვენი გასაღებით. ეს უნდა იყოს საიმედო პაროლი, შემდგარი არანაკლებ 8 სიმბოლოსაგან და არ უნდა შეიცავდეს არაალფაბეტურ სიმბოლოებს (წერტილი, მძიმე, ტირე..).



ნახ.3.11

გენერაციის წარმატებით დასრულების შემთხვევაში მივიღებთ შემდეგი სახის ფანჯარას იხილეთ ნახ.3.11.



ნახ.3.12

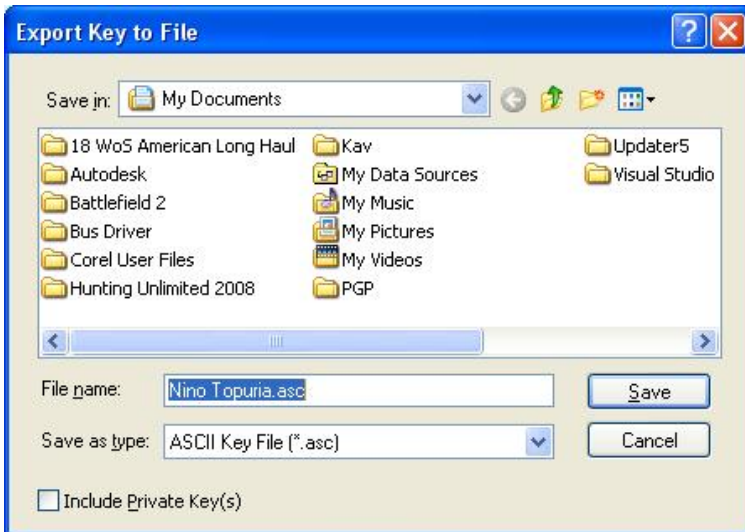
მას შემდეგ, რაც გენერაცია მშვიდობით დასრულდა შეგიძლიათ ინფორმაციის დაშიფრვა და დოკუმენტების ხელმოწერა.

ბოლოს ოსტატი გაძლევთ საშუალებას თუ გსურთ გაგზავნოთ ღია გასაღები გასაღებების სერვერზე (წინააღმდეგ შემთხვევაში აირჩიეთ Skip). იხილეთ ნახ.3.12

გასაღებების გავრცელება

გასაღებების მიღების შემდეგ (Public key და Private key) საჭიროა მათი გავრცელება. ყველაზე მოხერხებულია გასაღების გაგზავნა სერვერზე და თქვენი კორესპონდენტის გასაღების მიღება ასევე სერვერიდან.

საკუთარი ღია გასაღების სერვერზე გაგზავნა შეიძლება, როგორც ზემოთ იყო აღწერილი, გასაღების გენერაციის პროცესში. მეორე გზაა, აირჩიოთ ბრძანება Keys → Synchronize Selected Keys. ამის შემდეგ, ნებისმიერი მსურველი შეძლებს მის მიღებას, ეცოდინება რა თქვენი სახელი და ე-მეილი.



ნახ.3.13

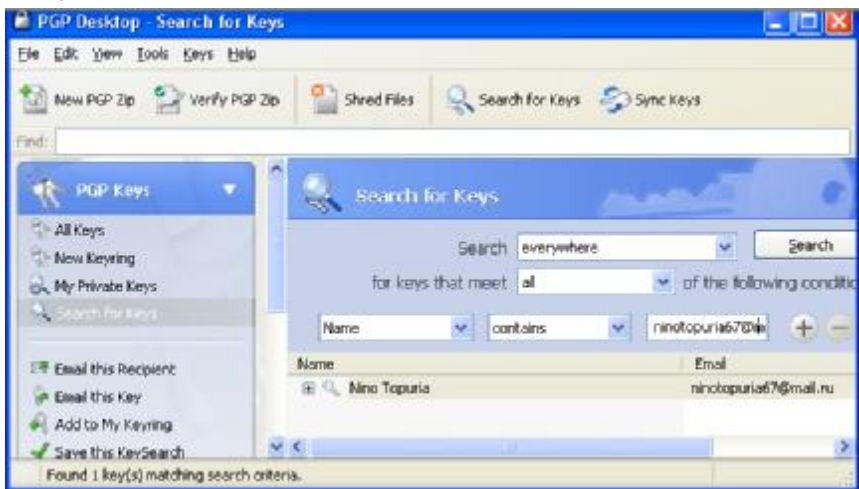
ღია გასაღები შეგიძლიათ გაუგზავნოთ იმ კონკრეტულ პირს, რომელთანაც აწარმოებთ მიმოწერას. აირჩიეთ ბრძანება File → Export. ეკრანზე გამოჩნდება ფანჯარა იხ.ნახ.3.13 არ მონიშნოთ

ოფცია Include Private Key(s), წინააღმდეგ შემთხვევაში გასაღების ექსპორტი მოხდება დახურულ გასაღებთან ერთად, მისი გაგზავნა კი არ არის საჭირო.

ამის შემდეგ მიუთითეთ საქალაქე და ფაილის სახელი, სადაც ინახავთ გასაღებს და მიაბით ეს ფაილი წერილის გაგზავნის დროს.

სერვერიდან გასაღების მისაღებად აირჩიეთ ბრძანება Search for Keys.

ეკრანზე გამოსულ ფანჯარაში მიუთითეთ ადრესატის ი-მეილი და დააჭირეთ ლილაკს Search. ამოარჩიეთ საჭირო გასაღები და მისი კონტექსტური მენიუდან აირჩიეთ ბრძანება Add to → New Keyring. იხილეთ ნახაზი 3.14.



ნახ.3.14

ინფორმაციის დაშიფრვა

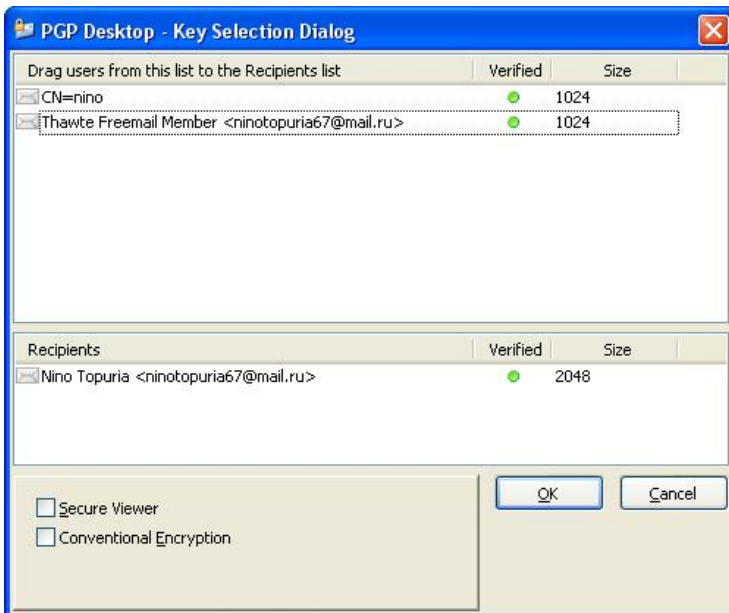
აკრიფეთ წერილის შინაარსი ნებისმიერ ტექსტურ რედაქტორში. ინფორმაციის დასაშიფრად შეასრულეთ შემდეგი მოქმედებები: ამოჭერთ ტექსტი და გადაიტანეთ გაცვლის ბუფერში ბრძანებით (Ctrl+X), Task bar-ზე გამოსახულ PGP-ის პიქტოგრამაზე დააჭირეთ თავის მარჯვენა ლილაკს და აირჩიეთ ბრძანება Clipboard→ Encrypt & Sign. იხილეთ ნახ.3.15.

ეკრანზე გამოჩნდება ფანჯარა იხილეთ ნახ. 3.16 აირჩიეთ საჭირო გასაღები და დააჭირეთ ლილაკს OK.

ახლა აირჩიეთ ბრძანება Clipboard → Edit, სადაც მოთავსებული იქნება დაშიფრული ინფორმაცია. იხილეთ ნახ. 3.15.



ნახ3.15.



ნახ3.16

აირჩიეთ ღილაკი Copy to Clipboard. ბრძანებით Ctrl+V გადაიტანეთ დამიფრული ინფორმაცია წერილში. ყოველივე ამის შემდეგ შეიძლება წერილის გაგზავნა



ნახ.3.17

3.6. დამიფრვის სხვა საშუალებები

ზემოაღწერილი საშუალებების გარდა არსებობს სხვა სასარგებლო უტილიტები უსაფრთხოების დასაცავად. ზოგი მათგანი უფასოა, ზოგი ფასიანი, სამაგიეროდ მომხმარებელს აღარ სჭირდება სერთიფიკატების მოთხოვნა და მათი მართვა. გთავაზობთ ზოგიერთი მათგანის მოკლე დახასიათებას.

CertifiedMail.com სამსახური

CertifiedMail.com სამსახური (<http://www.certifiedmail.com>)

შიფრაციისათვის იყენებს SSL ტექნოლოგიას. კომპანია ინახავს თქვენს თავდაპირველ შეტყობინებებს საკუთარ სერვერზე და ატყობინებს ამის შესახებ აღრესატებს ჩვეულებრივი ელექტრონული ფოსტის საშუალებით. აღრესატები უკავშირდებიან სერვერს SSL პროტოკოლით, შეჰყავთ პაროლი და იღებენ თავიანთ ფოსტას. ფოსტის გამგზავნი იღებს შტამპით დადასტურებულ შეტყობინებას

წერილის მიტანის შესახებ. სამსახურთან დაკავშირება შეიძლება საფოსტო კლიენტების Outlook, Outlook Express და Lotus Notes საშუალებით. სამსახური გთავაზობს სხვადასხვა დონის მომსახურებებს, როგორც ფასიანს ისე უფასოს.

HushMail სამსახური

HushMail სამსახური (<http://www.hushmail.com>) არის უფასო, ხოლო მისი მუშაობის წესები მოგვთავაზობს საფოსტო ვებ-სერვერების ფუნქციონირებას. მომხმარებელს შეუძლია HushMail-ში საკუთარი საფოსტო ყუთის დარეგისტრირება ნებისმიერი ვებ-ბროუზერით. ამის შემდეგ მას შეუძლია გაუგზავნოს დაშიფრული ან ხელმოწერილი შეტყობინება ადრესატს, რომელსაც ასევე ექნება შექმნილი საფოსტო ყუთი. სისტემა ფუნქციონირებს OpenPGP-ის სტანდარტზე.

იგი მოუხერხებლად შეიძლება ჩაითვალოს, რადგან შეტყობინების გასაგზავნად საჭიროა HushMail-ში დარეგისტრირება. თუმცა, მას აქვს უპირატესობა PGP-ისთან შედარებით – თქვენ შეგიძლიათ მიმართოთ საკუთარ საფოსტო ყუთს ნებისმიერი ადგილიდან.

PrivacyX სამსახური

PrivacyX სამსახური (<http://www.privacyx.com>) უზრუნველყოფს შიფრაციას და ანონიმურობას მუშაობისას. თქვენ გამოგეოფათ საფოსტო ყუთი და ციფრული სერთიფიკატი, რომელიც არ შეიცავს არანაირ ინფორმაციას თქვენს შესახებ. შეტყობინების გაგზავნა ხდება თქვენი PrivacyX საფოსტო ყუთის საშუალებით, ისე რომ გამოირიცხება ინფორმაცია იდენტიფიკაციის შესახებ (ადრესატი ვერ გეტყობს ვისგან არის გამოგზავნილი შეტყობინება). PrivacyX იყენებს S/MIME სტანდარტს, ამიტომ დასაშვებია, რომ თქვენი კორესპონდენტები არ იყვნენ რეგისტრირებულნი ამ სამსახურში.

სპამის თავიდან აცილების მიზნით ადრესატების რაოდენობა არ უნდა აღემატებოდეს 20. მომსახურება ფასიანია.

Sigaba Secure Email სამსახური

Sigaba Secure Email სამსახური (<http://www.sigaba.com>) უზრუნველყოფს საფოსტო შეტყობინებების შიფრაციას და გადასცემს “კომპიუტერიდან – კომპიუტერს”. ამ დროს გამოიყენება ვებ-ინტერფეისი ან სტანდარტული საფოსტო კლიენტ-პროგრამები.

(Outlook, Outlook Express, Lotus Notes, Eudora და Novell GroupWise, ასევე Hotmail და Yahoo Mail) Sigaba Secure Email სამსახური იყენებს სიმეტრიულ და დახურულ გასაღებებს, ასევე გასაღებებს შეტყობინებების ხელმოსაწერად და არა მომხმარებელთა იდენტიფიკაციის საშუალებებს. სერვისის გამოსაყენებლად გამგზავნი და ადრესატი უნდა დარეგისტრირდნენ სამსახურში. მომსახურება უფასოა.

ZixMail სამსახური

ZixMail სამსახური (<http://www.zixit.com>) უფლებას აძლევს მოახდინონ ელექტრონული შეტყობინებების დაშიფრვა და ხელმოწერა, როგორც სამსახურში დარეგისტრირებულ, ისე არადარეგისტრირებულ მომხმარებლებს. დარეგისტრირებული მომხმარებლები ღებულობენ ფოსტას ელექტრონული წერილის სახით, ხოლო არადარეგისტრირებულები მიიღებენ შეტყობინებას, რომ მათთვის განკუთვნილი უსაფრთხო წერილი იმყოფება ZixMail-სერვერზე. ამ დროს სერვერთან დაკავშირება ხორციელდება SSL დონეზე.

სამსახურთან დაკავშირება შესაძლებელია საფოსტო კლიენტების (Outlook და Lotus Notes) საშუალებით. მომსახურება ფასიანია.

საკონტროლო კითხვები:

1. როგორ მოახდინოთ უსაფრთხოების ზონების კონფიგურაციების დაყენება Internet Explorer-ში?
2. როგორ მივიღოთ ციფრული სერთიფიკატი?
3. როგორ გავუგზავნოთ ღია გასაღები ადრესატს?
4. როგორ გავაგზავნოთ წერილი ხელმოწერილი ციფრული სერთიფიკატით?
5. როგორ გავაგზავნოთ S/MIME ფორმატით დაშიფრული შეტყობინება?
6. როგორ გავაგზავნოთ დაშიფრული შეტყობინება PGP-ის საშუალებით?

თავი 4. ფაილებისა და საქალაქდების კოდირება

4.1. მონაცემების კოდირება

კოდირებული ფაილური სისტემა (Encrypting File System, EFS), საშუალებას იძლევა დაშიფროთ ფაილები, რომლებიც მოთავსებულია NTFS ტომებში და შესაბამისად უზრუნველყოფს მონაცემთა უსაფრთხო შენახვას. EFS-ი არის უსაფრთხოების კიდევ ერთი დონე მიმართვის უფლებებთან ერთად, რომელიც არსებობს NTFS სისტემაში. თუმცა მას აქვს თავისი “სუსტი ადგილები”. ყველა მომხმარებელს, რომელსაც აქვს ადმინისტრატორის მიმართვის უფლება, შეუძლია მიმართოს თქვენს ფაილს.

კოდირებისას Windows ოპერაციული სისტემა იყენებს შემთხვევითი რიცხვების გენერატორს, ქმნის ფაილების კოდირების გასაღებს (File encryption key, FEK), და შემდგომ იყენებს მათ კოდირებისათვის. ამის შემდეგ, ხდება თვით FEK გასაღების კოდირება ღია გასაღების საშუალებით. გასაღების დეკოდირებისათვის აუცილებელია სერთიფიკატი და მასთან ასოცირებული ღია გასაღები, რომელთან მიმართვაც მომხმარებელს სახელისა და პაროლის მითითების შემდეგ შეუძლია. ყველა სხვა მომხმარებელი, რომელიც ეცდება კოდირებულ ფაილებთან მუშაობას, მიიღებს შეტყობინებას “access denied”. ადმინისტრატორის უფლებების მქონე მომხმარებელიც კი ვერ წაიკითხავს თქვენს მონაცემებს.

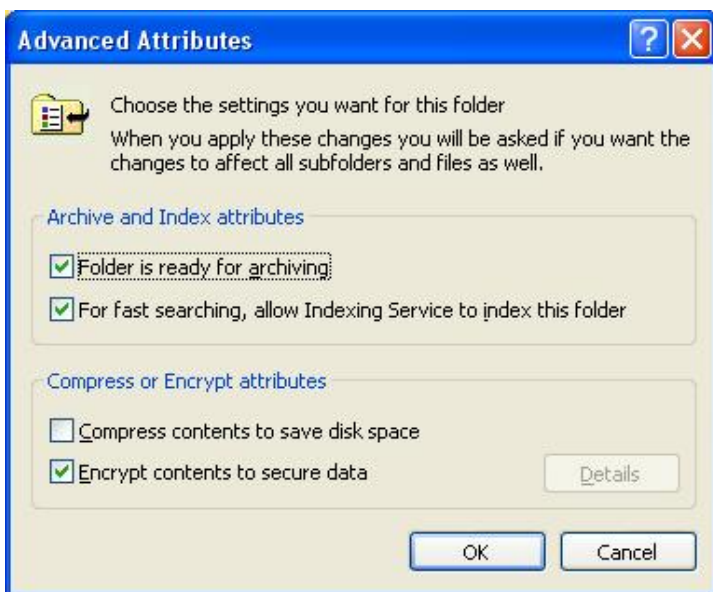
შესაძლებელია ცალკეული ფაილების, საქალაქდების ან მთელი დისკების კოდირება. რეკომენდებულია არა ცალკეული ფაილების, არამედ მთელი საქალაქდების კოდირება. კოდირებული საქალაქდის შემთხვევაში, ახლად შექმნილი ფაილების კოდირება ხდება ავტომატურად.

საქალაქდის კოდირებისათვის აირჩიეთ შემდეგი მოქმედებები:

1. მონიშნეთ საქალაქდე, მისი კონტექსტური მენიუდან აირჩიეთ Properties, შემდეგ ჩანართი General და ლილაკი Advanced. (იხილეთ ნახ4.1).

2. აირჩიეთ ოფცია და დააჭირეთ ლილაკს OK.

დეკოდირებისათვის მოხსენით ალამი ოფციაზე Encrypt contents to secure data.



ნახ.4.1.

კოდირება Cipher ბრძანებით

კოდირება Cipher წარმოადგენს ალტერნატიულ უტილიტას, რომელიც მუშაობს ბრძანებათა სტრიქონის რეჟიმში და ემსახურება ფაილების კოდირება/დეკოდირებას.

ცხრილში მოცემულია Cipher პროგრამის ზოგიერთი პარამეტრიც. სრული სიის დასათვალიერებლად ბრძანებათა სტრიქონში აკრიფეთ cipher /?

გასაღები	აღწერა
/E	მითითებული საქაღალდეების კოდირება
/D	მითითებული საქაღალდეების კოდირება
/S:საქაღალდე	საქაღალდეებსა და ქვესასაქაღალდეებზე (და არა ფაილებზე) ოპერაციების შესრულება
/A	ოპერაციების შესრულება მითითებულ ფაილებზე

მაგალითად, მოვახდინოთ My Documents საქალაქის კოდირება მასში არსებულ ფაილებთან და ქვესაქალაქებთან ერთად. ბრძანებათა სტრიქონში აირჩიეთ:

cipher /e/a/s: "%userprofile%\my documents"

ფაილის აღდგენის სერთიფიკატის შესაქმნელად შესრულეთ შემდეგი მოქმედებები:

- დარეგისტრირდით სისტემაში ადმინისტრატორის უფლებებით
- ბრძანებათა სტრიქონში აკრიფეთ cipher /r:Filename, სადაც Filename არის იმ ფაილის სახელი, რომელიც უნდა მიანიჭოთ სერთიფიკატის ფაილს.
- აკრიფეთ პაროლი, რომელიც შემდგომში გამოიყენება თქვენს მიერ შექმნილი ფაილების დასაცავად. შეიქმნება ფაილები გაფართოებით .pfx და .cer.

კოდირებული ფაილების იდენტიფიცირება

ქვემოთ ჩამოთვლილია მეთოდები, რომელთა საშუალებითაც გაარკვევთ კოდირებულულია თუ არა მოცემული ფაილი (საქალაქად).

- Windows XP, გაჩუმების პრინციპით, კოდირებულ ფაილებს გამოყოფს მწვანე ფერით.
- ბრძანებათა სტრიქონში აკრიფეთ cipher ბრძანება პარამეტრების მითითების გარეშე. კოდირებული ფაილების წინ წერია სიმბოლო "f", ხოლო ჩვეულებრივი ფაილების წინ წერია სიმბოლო "U".
- ყველა კოდირებული ფაილის სიის ეკრანზე გამოსატანად, ბრძანებათა სტრიქონში აკრიფეთ cipher /u /n.

კოდირებულ და ჩვეულებრივ ფაილებს შორის არსებობს ძნელად შესამჩნევი, მაგრამ მნიშვნელოვანი განსხვავებები.

- თუ სისტემაში დარეგისტრირდებით ისეთი აღრიცხვის ჩანაწერით, რომლითაც არ იყო კოდირებული ფაილი, მაშინ ასეთი ფაილის გახსნის მცდელობისას სისტემას გამოაქვს შეტყობინება "access denied". იგივე შეტყობინება გამოვა ასეთი ფაილის დეკოდირების მცდელობისას. მომხმარებელს, რომელსაც აქვს ფაილების შეცვლის უფლება, შეუძლია წაშალოს ან სახელი გადაარქვას კოდირებულ ფაილს.

- თუ მოახდენთ ჩვეულებრივი ფაილის გადატანას კოდირებულ საქალაქში, ამ ფაილის ასლი მოცემულ საქალაქში იქნება კოდირებული.

- თუ სახელს გადაარქმევთ კოდირებულ ფაილს, იგი კვლავ რჩება კოდირებული.

- თუ წაშლით კოდირებულ ფაილს, კალათიდან (Recycle Bin) აღდგენილი ფაილი კვლავ იქნება კოდირებული.

- თუ გსურთ იმუშაოთ დაშიფრულ ფაილთან სხვა კომპიუტერზე, თქვენი პერსონალური სერტიფიკატი და მისი კუთვნილი დანურული გასაღები უნდა არსებობდეს ამავე კომპიუტერზე. შესაძლებელია გასაღებების კოპირებაც.

იმისათვის, რომ გაარკვიოთ თუ ვის მიერაა კოდირებული ესა თუ ის ფაილი და რომელ მომხმარებელს აქვს დეკოდირების უფლება არსებობს საშუალება Efsinfo.exe, რომლის გადმოტვირთვაც შეიძლება Microsoft-ის სერვერიდან <http://www.reskits.com>.

EFS დაცვის გაძლიერება

EPS ფაილური სისტემა უზრუნველყოფს დაცვის საიმედო დონეს. გაჩემების პრინციპით, კოდირება/დეკოდირებისათვის გამოიყენება მონაცემთა კოდირების გაფართოებული სტანდარტი (Data Encryption Standart, DESX). Windows XP-ში არსებობს საშუალება კიდევ უფრო აამაღლოთ უსაფრთხოების დონე მონაცემთა სამმაგი კოდირების სტანდარტის (Triple Data Encryption Standart, 3DES) გამოყენების საშუალებით.

3DES-ის ჩასართავად შეასრულეთ შემდეგი ბრძანებები:

1. გააქტიურეთ კონსოლი Local Security Settings (Secpol.msc).
2. ამორჩიეთ განყოფილება Security Settings\Local Policies\Security Options.
3. ამორჩიეთ პუნქტი System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, And Signing.
4. აირჩიეთ რეჟიმი Enabled და დააჭირეთ კლავიშას OK.

4.2. მონაცემების აღდგენის აგენტის დანიშვნა

ერთ-ერთი მომხმარებლის დანიშვნა მონაცემების აღდგენის აგენტად, საშუალებას მოგცემთ აღადგინოთ კოდირებული ფაილები დაზარული გასაღების დაკარგვის შემთხვევაში.

აღდგენის სერთიფიკატის შექმნა

აღდგენის სერთიფიკატის შესაქმნელად შეასრულეთ შემდეგი მოქმედებები:

1. დარეგისტრირდით სისტემაში ადმინისტრატორის უფლებებით
2. ბრძანებათა სტრიქონში აკრიფეთ cipher /r:filename, სადაც filename – სახელია, რომელსაც არქმევთ სერთიფიკატის ფაილს. გაფართოების მითითება არ არის საჭირო.

3. აკრიფეთ პაროლი, რომელსაც გამოიყენებთ თქვენს მიერ შექმნილი ფაილების დასაცავად.

ბრძანების შესრულების შემდეგ შეიქმნება ფაილები გაფართოებით .pfx და .cer.

მონაცემების აღდგენის აგენტების დანიშვნა

აგენტის სტატუსი შეგიძლიათ მიანიჭოთ ნებისმიერ მომხმარებელს.

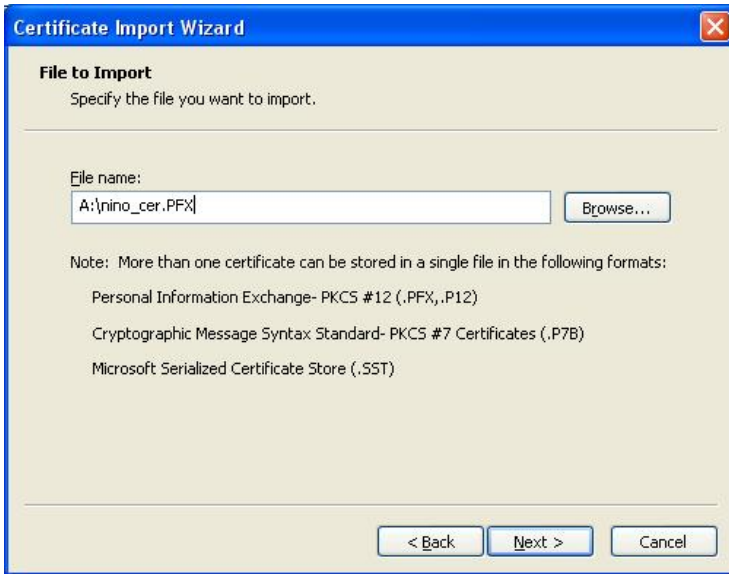
1. დარეგისტრირდით სისტემაში იმ აღრიცხვის ჩანაწერით, ვისაც გსურთ მიანიჭოთ აგენტის ფუნქციები.

2. აირჩიეთ ბრძანება certmgr.msc და გადადით განყოფილებაში Certificates-Current User\Personal.

3. შეასრულეთ ბრძანება Action→All Tasks→Import, რის შემდეგაც გაეშვება Certificate Import Wizard. დააჭირეთ ღილაკს Next.

4. აკრიფეთ კოდირების სერთიფიკატის ფაილის სახელი და გზა (ფაილი გაფართოებით .pfx), რომელიც ექსპორტირებული იყო ადრე (იხილეთ ნახ.4.2) და დააჭირეთ ღილაკს Next. Browse ღილაკს დაჭერის შემდეგ, Files of Type ველში აირჩიეთ პუნქტი Personal Information Exchange, რათა მოძებნოთ ფაილები გაფართოებით .pfx. დააჭირეთ ღილაკს Next.

5. მიუთითეთ პაროლი თქვენი სერთიფიკატისათვის და აირჩიეთ ოფცია Mark This Key As Exportable. დააჭირეთ ღილაკს Next.



ნახ.4.2

6. აირჩიეთ პარამეტრი Automatically Select The Certificate Store On The Type Of Certificate და კვლავ დააჭირეთ ლილაკს Next.

7. აირჩიეთ ბრძანება secopl.msc და გადადით განყოფილებაში Security Settings→Public Key Policies→Encrypting File System.

8. აირჩიეთ ბრძანება Action→Add Data Recovery Agent. დააჭირეთ ლილაკს Next.

9. Add Recovery Agent Wizard ფანჯარაში, აირჩიეთ ლილაკი Browse და მოძებნეთ ის საქალაქო, რომელიც შეიცავს თქვენს მიერ შექმნილ ფაილს გაფართოებით .cer. ამოირჩიეთ ფაილი და დააჭირეთ ლილაკს Open.

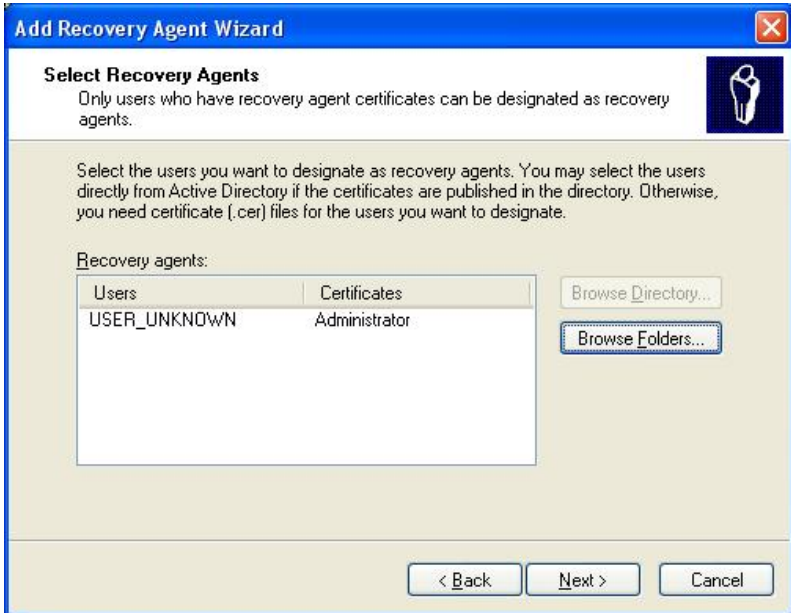
10. Add Recovery Agent Wizard ფანჯარაში გამოჩნდება ახალი აგენტი USER_UNKNOWN. (იხილეთ ნახ.4.3).

ამგვარად, მიმდინარე მომხმარებელი დანიშნულია მონაცემების აღდგენის აგენტად სისტემაში კოდირებული ყველა ფაილებისათვის.

დახურული გასაღების წაშლა

იმისათვის, რათა აღკვეთოთ სიტუაცია, როდესაც რომელიმე მომხმარებელი დარეგისტრირდება სისტემაში ადმინისტრატორის

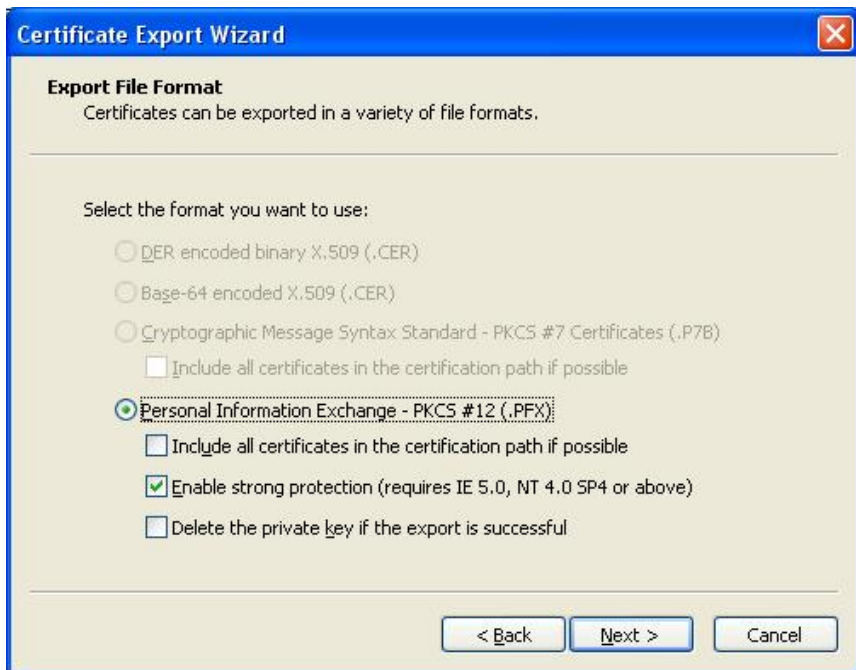
აღრიცხვის ჩანაწერთ (ან მონაცემების აღდგენის აგენტის აღრიცხვის ჩანაწერთ) და შეძლებს სხვა მომხმარებლების მიერ კოდირებული ფაილების დათვალიერებას, საჭიროა კერძო გასაღების წაშლა ან მათი ექსპორტის განხორციელება.



ნახ.4.3

აგენტის გასაღების წაშლელად შესრულოთ შემდეგი მოქმედებები:

1. დარეგისტრირდით სისტემაში მონაცემების აღდგენის აგენტის აღრიცხვის ჩანაწერთ.
2. აირჩიეთ ბრძანება აირჩიეთ ბრძანება certmgr.msc და გადადით განყოფილებაში Certificates-Current User\Personal.
3. მონიშნეთ File Recovery სერთიფიკატი, დააჭირეთ თავუს მარჯვენა ღილაკს და აირჩიეთ ბრძანება All Tasks→Export. ეკრანზე გაეშუება Certificate Export Wizard - ოსტატი. დააჭირეთ ღილაკს Next.
4. დააჭირეთ ღილაკს Yes, შემდეგ ღილაკს Export The Private Key და Next.



ნახ.4.4

4. აირჩიეთ პუნქტი Enable Strong Protection და Delete The Private Key if The Exports Is Successful იხილეთ ნახ.4.4, დააჭირეთ ღილაკს Next.
5. ორჯერ აკრიფეთ პაროლი და კვლავ დააჭირეთ ღილაკს Next.
6. აკრიფეთ სახელი და გზა ექსპორტირებულ ფაილამდე.
7. დააჭირეთ ღილაკს Next და Finish.

ისევე, როგორც სერთიფიკატების შემთხვევაში, აუცილებელია ფაილის კოპირება დისკეტზე (რომელიც ინახება დაცულ ადგილას), და შემდეგ მისი წაშლა მყარი დისკიდან.

ამრიგად, რადგან დახურული გასაღები მიულწევადია, აგენტი ვერ შეძლებს კოდირებული ფაილების შემცველობის დათვალიერებას. იმისათვის, რომ აგენტმა შეძლოს კოდირებულ ფაილებთან მიმართვა, აუცილებელი იქნება დახურული გასაღების იმპორტი.

4.3. სერთიფიკატების სარეზერვო კოპირება

როდესაც მონაცემების კოდირება ხდება პირველად, Widows-ი ქმნის “საკუთარ” სერთიფიკატს EFS-ისათვის. სიტყვა “საკუთარი” ნიშნავს, რომ სერთიფიკატი არ არის გაცემული რომელიმე ორგანიზაციის მიერ. ეს სერთიფიკატი ხდება თქვენი კოდირების პერსონალური სერთიფიკატი. მასში მოთავსებულია გასაღებები (ღია და დახურული), რომლებიც აუცილებელია ფაილების კოდირება/დეკოდირების ოპერაციების შესასრულებლად.

თითოეული მომხმარებელი, რომელიც ახორციელებს ფაილების კოდირება/დეკოდირებას, ღებულობს საკუთარ პერსონალურ სერთიფიკატს.

თითოეულ მომხმარებელს შეუძლია თავისი სერთიფიკატების კოპირება შემდგომი შენახვის მიზნით. ფაილების აღდგენის სერთიფიკატი, საშუალებას აძლევს სისტემურ ადმინისტრატორს, მიმართოს მონაცემებს იმ შემთხვევაში, თუ მომხმარებლის პერსონალური სერთიფიკატი მიუღწევადია.

სერთიფიკატის სარეზერვო კოპირების განსახორციელებლად, შეასრულეთ შემდეგი მოქმედებები:

1. დარეგისტრირდით სისტემაში, როგორც Administrators ჯგუფის წევრი.
2. ბრძანებათა სტრიქონში აირჩიეთ ბრძანება Secpol.msc, აირჩიეთ ბრძანება Security Settings → Public Key Policies\Encrypting File System.
3. აირჩიეთ ადმინისტრატორის სერთიფიკატი, დააჭირეთ თავუს მარჯვება ღილაკს და აირჩიეთ ბრძანება All Tasks → Export. ეკრანზე გამოჩნდება სერთიფიკატების ექსპორტის ოსტატი. აირჩიეთ ღილაკი Next.
4. ამოირჩიეთ ოფცია DER Encoded Binary X.509(CER.) იხილეთ ნახ.4.5.
5. მიუთითეთ ექსპორტისათვის განკუთვნილი ფაილის სახელი და გზა, დააჭირეთ ღილაკს Finish.



ნახ.4.5

კოდირების პერსონალური სერთიფიკატების ექსპორტი

პერსონალური სერთიფიკატების კოდირებისათვის შეასრულეთ შემდეგი ბრძანებები:

1. დარეგისტრირდით სისტემაში იმ მომხმარებლის აღრიცხვის ჩანაწერით, რომლის სერთიფიკატის კოდირებასაც აპირებთ.
2. გააქტიურეთ Internet Explorer-ი და აირჩიეთ ბრძანება Tools→Internet Options→Contents→Certificates.
3. ამოირჩიეთ ის სერთიფიკატი, რომლის თვისებებშიც მითითებულია Encrypting File System და აირჩიეთ ღილაკი Export. იხილეთ ნახ.3.7.
4. ეკრანზე გამოჩნდება ოსტატი (Certificates Export Wizard). დააჭირეთ ღილაკს Next.
5. აირჩიეთ ოფცია Export The Private Key და ორჯერ დააჭირეთ ღილაკს Next.

6. აკრიფეთ პაროლი .pfx გაფართოების მქონე ფაილისათვის. იგი არ უნდა ემთხვეოდეს აღრიცხვის ჩანაწერის პაროლს. დააჭირეთ ღილაკს Next.
7. მიუთითეთ ექსპორტისათვის განკუთვნილი ფაილის სახელი და გზა.
8. დააჭირეთ ღილაკს Next და Finish.

კოდირების პერსონალური სერთიფიკატების იმპორტი

საკუთარი პერსონალური სერთიფიკატის იმპორტი შეიძლება დაგჭირდეთ შემდეგ შემთხვევებში:

- თუ გსურთ კოდირებულ ფაილებთან მუშაობა სხვა კომპიუტერზე;
- თუ თქვენი პერსონალური კომპიუტერი დაიკარგა ან დაზიანდა.

სერთიფიკატის იმპორტისათვის შეასრულეთ შემდეგი ოპერაციები.

1. გააქტიურეთ Internet Explorer-ი და აირჩიეთ ბრძანება Tools→Internet Options→Contents→Certificates
2. დააჭირეთ ღილაკს Import, ეკრანზე გაეშვება Certificates Import Wizard (ოსტატი).
3. აკრიფეთ სახელი და გზა სერთიფიკატამდე (ფაილი გაფართოებით .pfx), რომლის ექსპორტირებაც ადრე მოხდა.
4. აკრიფეთ პაროლი, აუცილებლობის შემთხვევაში აირჩიეთ პარამეტრები და დააჭირეთ ღილაკს Next.
5. ამორჩიეთ ოფცია Place All Certificates In The Following Store, დააჭირეთ ღილაკს Browse, აირჩიეთ პუნქტი Personal. დააჭირეთ ღილაკებს OK, Next და Finish.

კოდირების ახალი პერსონალური სერთიფიკატის შექმნა

საკუთარი პერსონალური სერთიფიკატის დაკარგვის შემთხვევაში Cipher.exe პროგრამა, საშუალებას მოგცემთ შექმნათ ახალი სერთიფიკატი. ამისათვის ბრძანებათა სტრიქონში აკრიფეთ cipher /k.

აღსანიშნავია, რომ ახალი სერთიფიკატის გამოყენებას ვერ შეძლებთ იმ ფაილების დეკოდირებისათვის, რომლებიც კოდირებულია ძველი სერთიფიკატის გასაღებით.

თავი 5. მონაცემების დაცვა

5.1. მონაცემების სარეზერვო ასლების შექმნა

ინფორმაციის დაცვის თვალსაზრისით, აღსანიშნავია მონაცემთა სარეზერვო ასლების შექმნა, რაც გამოორიცხავს მნიშვნელოვანი ინფორმაციის დაკარგვის საშიშროებას. მონაცემთა დაკარგვის პოტენციური საფრთხეებია:

- მყარი დისკის დაზიანება. დღესდღეობით მყარი დისკები იმდენად სანდოა, როგორც არასდროს. თუმცა, ვერ გამოვრიცხავთ ისეთ ფაქტორებს როგორცაა: დავარდნა, კომპიუტერის ვიბრაცია ან ენერგომომარაგებით გამოწვეული პრობლემები (ძაბვის ვარდნა აზიანებს ვინჩესტერს);

- ხანძარი, წყალდიდობა, მიწისძვრა და სხვა სტიქიური უბედურებები;

- ქურდობა. ამ მხრივ აღსანიშნავია პორტატული კომპიუტერები;

- მომხმარებელთა შეცდომები. შემთხვევით წაშლილი ფაილები.

Windows-ის შემადგენლობაში შედის სარეზერვო ასლის შექმნის პროგრამა Windows Backup.

არსებობს მონაცემების სარეზერვო ასლების შექმნის სხვადასხვა ტიპები. ყველაზე მეტად გავრცელებლია Normal (ნორმალური ანუ სრული), Incremental (დამატებითი) და Differential (დიფერენცირებული) სარეზერვო ასლები.

Normal backup-ი ახდენს მონაცემების სრული რეზერვის შექმნას. მაგალითად, გვაქვს 10 ფაილი. Normal backup-ის შესრულების შემდეგ მიიღება კვლავ 10 ფაილი.

Incremental backup-ის შესრულება შეიძლება მხოლოდ Normal backup-ის შესრულების შემდეგ. Incremental backup-ი ახდენს იმ ფაილების სარეზერვო ასლების შექმნას, რომელთა შეცვლაც Normal backup-ის უკანასკნელი შესრულების შემდეგ მოხდა. მაგალითად, გვქონდა 10 ფაილი, შეიცვალა 1 ფაილი, Incremental backup-ის შესრულების შემდეგ მივიღებთ 1 ფაილს, შემდგომში თუ მოხდა კიდევ 1 ფაილის შეცვლა, მივიღებთ 10+1+1 ფაილს (აქედან 10 Normal backup-ის და 2 Incremental backup-ის ფაილებია). იმ ფაილებისათვის, რომლებიც არ შეცვლილან, Incremental backup-ის შესრულება არ მოხდება.

Differential backup-ის შესრულება ხდება უკანასკნელი Normal backup-ის შესრულების მომენტიდან. მაგალითად, გვქონდა Normal backup-ის 10 ფაილი, შეიცვალა 1 ფაილი, შესრულდა differential backup-ი 1 ფაილისათვის, მეორე დღეს შეიცვალა კიდევ ორი, შესრულდა differential backup-ი 2 ფაილისათვის. ჯამში მიიღება Normal backup-ის 10 ფაილი, 1 დღეს – 1 ფაილი, მეორე დღეს 2 ფაილი.

ამგვარად, Incremental backup-ი მოითხოვს ცოტა დროს შექმნაზე, მაგრამ დიდ დროს აღდგენისათვის. Differential backup-ი მოითხოვს დიდ დროს სარეზერვო ასლის შექმნაზე და ცოტა დროს აღდგენაზე. Incremental backup-ის შემთხვევაში უნდა აღდგეს მთელი ჯაჭვი, ხოლო Differential backup-ის დროს მხოლოდ Normal backup-ი და უკანასკნელი Differential backup-ი.

მოვიყვანოთ მაგალითი. განვიხილოთ აფთიაქის მონაცემთა ბაზა. კვირას ხდება მონაცემთა ბაზის Normal backup-ის შესრულება, Incremental backup-ის შესრულებისას ორშაბათიდან შაბათის ჩათვლით მიიღება 6 ფაილი. თუ საჭიროა ბაზის მდგომარეობის ნახვა ოთხშაბათისათვის, უნდა აღდგეს Normal backup + ორშაბათის Incr. backup + სამშაბათის Incr. backup + ოთხშაბათის Incr. backup-ი. იმ შემთხვევაში, თუ იყო შესრულებული Differential backup-ი ყოველდღე, მაშინ ოთხშაბათის სანახავად უნდა აღდგეს Normal backup + ოთხშაბათის Differential backup-ი.

ფაილების სარეზერვო ასლების შექმნის საერთო სტრატეგია გულისხმობს იმას, რომ პერიოდულად შესრულდეს კომპიუტერის მყარ დისკზე არსებული მთელი ინფორმაციის სრული ასლის კოპირება. თუ თქვენ იყენებთ კომპიუტერს ყოველდღე, უმჯობესია შექმნათ მონაცემების სრული სარეზერვო ასლი ყოველკვირა; მომხმარებელი, რომელიც იშვიათად იყენებს კომპიუტერს, შეუძლია შეასრულოს სრული სარეზერვო კოპირება თვეში ერთხელ.

სარეზერვო ასლების შენახვა შესაძლებელია ინფორმაციის შემდეგ დამგროვებლებზე:

- დისკეტები. მათი ზომა 1.44 მგ-ია. გამოიყენება მაშინ, თუ სხვა ალტერნატივა არარსებობს;

- zip-დისკები (მოცულობით 100 და 250 მგ) და ჯაზ-დისკები (მოცულობით 1 და 2 გბიტ) სასურველია მათი გამოყენება, მაგრამ ძალიან ძვირია;

– მაგნიტოოპტიკური დისკები (MO), მოცულობით 128 მგბატიდან 5 გბაიტამდე.

– მაგნიტური ლენტა. მაგნიტური ლენტების კასეტები არსებობს სხვადასხვა მოცულობის. რადგან სარეზერვო ასლის შექმნა ხანგრძლივი პროცესია, საჭირო ხდება რამოდენიმე კასეტის გამოყენება, ხოლო სტრიმერები საკმაოდ ძვირია.

– მყარი დისკი. სარეზერვო ასლის შექმნა სხვა მყარ დისკზე, ხშირად ყველაზე უფრო მოსახერხებელია, რადგან ამ შემთხვევაში პროცესი შეიძლება განხორციელდეს ავტომატურ რეჟიმში. თუმცა სარეზერვოდ მყარი დისკის გამოყენებაც ძვირი სიამოვნებაა.

– კომპაქტ დისკი CD-RW. ფასის მხრივ ხელმისაწვდომია, მაგრამ მოცულობის (650მგ) გამო საჭიროა რამოდენიმე კომპაქტ-დისკის გამოყენება.

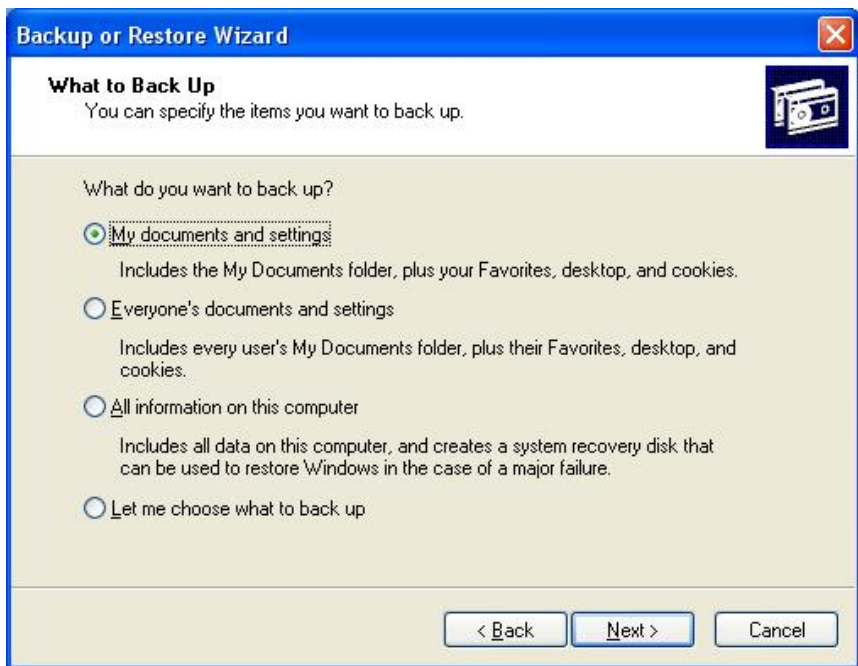
– საცავი დაფუძნებული ვებ-ტექნოლოგიებზე. არსებობს კომპანიები, რომლებიც გთავაზობენ მსგავს მომსახურებას ინტერნეტში. მაგალითად, სარეზერვო ასლის შექმნელი პროგრამა SwapDrive, მისამართზე <http://www.swapdrive.com>. მაგრამ ინტერნეტში ჩქარი და საიმედო ჩართვის შემთხვევაშიც კი რამოდენიმე გიგაბაიტი მოცულობის მონაცემების ასლის შექმნა დიდ დროს საჭიროებს. ამას გარდა, მსგავსი ტექნოლოგიით შენახულ ასლებს ვერ მიმართავთ იმ შემთხვევაში თუ კომპიუტერი გაფუჭდა (სანამ არ აღადგენთ მას) ან მოიპარეს. დაწვრილებითი ინფორმაცია იხილეთ საიტზე <http://dir.yahoo.com>

– უნივერსალური ციფრული დისკი DVD. დიდი მოცულობის გამო 9.4 გბაიტი მეტად მოხერხებულად შეიძლება ჩაითვალოს.

აღსანიშნავია, რომ Windws Backup-ს არ შეუძლია ასლების შექმნა CD-R და CD-RW-ზე. ამ შემთხვევაში სარეზერვო ასლი ჯერ უნდა შეიქმნას მყარ დისკზე, ხოლო შემდეგ ჩაიწეროს კომპაქტ-დისკზე. პროგრამებს Drive Image5 და Norton Ghost 2002 შეუძლიათ შექმნან ასლები პირდაპირ კომპაქტ-დისკებზე.

ყოველდღიური სარეზერვო ასლების შესაქმნელად შეასრულეთ შემდეგი მოქმედებები:

1. Windows Backup-ის გასააქტიურებლად შეასრულეთ ბრძანება Start → Programs → Accessories → System Tools → Backup ან ბრძანებთა სტრიქონში აირჩიეთ ბრძანება ntbackup. ეკრანზე გამოჩნდება ოსტატი;



ნახ.5.1

2. აირჩიეთ **Back up files and settings**; იხილეთ ნახ.5.1.

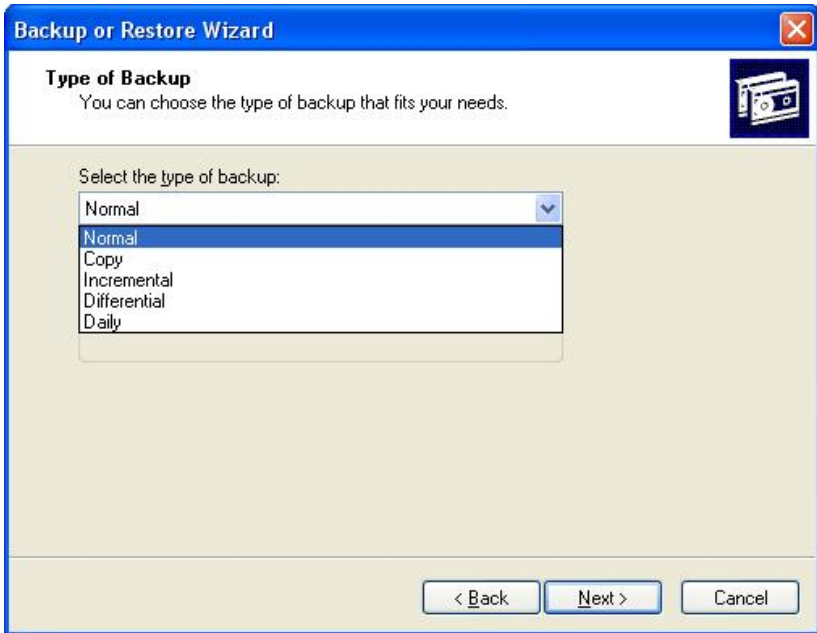
3. აირჩიეთ **My documents and settings** ან **Everyone's documents and settings**. ეს ოფციები შეიცავს მნიშვნელოვან ფაილებს თქვენი პროფილიდან და გამორიცხავენ მთელ რიგ ისეთ ფაილებს, რომელთა სარეზერვო ასლების შექმნა არ არის საჭირო. დააჭირეთ ღილაკს **Next**.

4. აირჩიეთ **საქალაქე**, სადაც აპირებთ სარეზერვო ასლის შენახვას. დააჭირეთ ღილაკს **Next**.

5. ბოლო ბიჯზე არსებული ღილაკი **Advanced**, საშუალებას იძლევა აირჩიოთ სარეზერვო ასლის ტიპი იხილეთ ნახ.5.2. და დააყენოთ გრაფიკი თქვენი ამოცანისათვის.

6. ოფცია **Append this backup to the existing backups** – მიუმატებს სარეზერვო ასლებს უკვე არსებულ რეზერვს.

7. ოფცია **Replace the existing backup** – შეცვლის უკვე არსებულ რეზერვს.



ნახ.5.2

ოფცია Allow only the owner and the Administrator access to the backup data and to any backups appended to the medium – უფლებას აძლევს Administrators ჯგუფის წევრებს აღადგინოს ფაილები თქვენი სარეზერვო ფაილიდან. ეს ოფცია იცავს იმ მომხმარებლისაგან, რომელთაც არ აქვთ აღრიცხვის ჩანაწერი თქვენს კომპიუტერზე და სურთ ამ ფაილის გამოყენება. იხილეთ ნახ.5.3.

ლილაკი Schedule, საშუალებას გაძლევთ შეადგინოთ გრაფიკი, სადაც დაგეგმავთ სარეზერვო ასლების შექმნის ამოცანის გაშვებას ნებისმიერი დროსათვის.

5.2. მონაცემთა დაცვის სხვა საშუალებები

Windows-ის შემადგენლობაში შედის რამოდენიმე უტილიტა, რომლებიც მონაცემთა დაცვის საშუალებას იძლევიან.

უტილიტა Chkdsk.

უტილიტა Chkdsk-ი ახდენს დისკის შემოწმებას, ეძებს შეცდომებს სისტემურ ფაილებში და მონაცემთა მატარებლებზე.



ნახ.5.3

აირჩიეთ დისკი რომლის შემოწმებაც გინდათ, მისი კონტექსტური მენიუდან აირჩიეთ Properties→Tools→Check. დიალოგურ ფანჯარაში გამოჩნდება ორი ოფცია (იხილეთ ნახ.5.4.):

Automatically fix file system errors – შეცდომების ავტომატური შესწორება ფაილურ სისტემაში. (ექვივალენტური ბრძანებაა Run→Chkdsk/F).

Scan For and Attempt Recovery Of Bad Sectors – სკანირება და დაზიანებული სექტორების კორექტირების მცდელობა (ექვივალენტური ბრძანებაა Run→Chkdsk/R). ამ უტილიტის დამატებითი ბრძანების სანახავად აირჩიეთ ბრძანება chkdsk/?.



ნახ.5.4

System Restore

System Restore უტილიტა თვალს ადევნებს სისტემაში მომხდარ ცვლილებებს. იგი დღეში ერთხელ ავტომატურად ქმნის სისტემური ფაილებისა და სისტემური რეესტრის მონაცემების ასლებს, რომლებსაც ინახავს ფარულ არქივში. System Restore-ი ქმნის დაბრუნების წერტილებს შემდეგი მოქმედების შესრულების შემთხვევაში:

- თუ ხორციელდება მოწყობილობის არასაშტატო დრაივერის ინსტალაციის მცდელობა, Windows-ს ეკრანზე გამოაქვს გამაფრთხილებელი შეტყობინება. მუშაობის გაგრძელების შემთხვევაში System Restore-ი ქმნის დაბრუნების წერტილს, მანამ სანამ გააგრძელებს ინსტალაციის პროცესს.

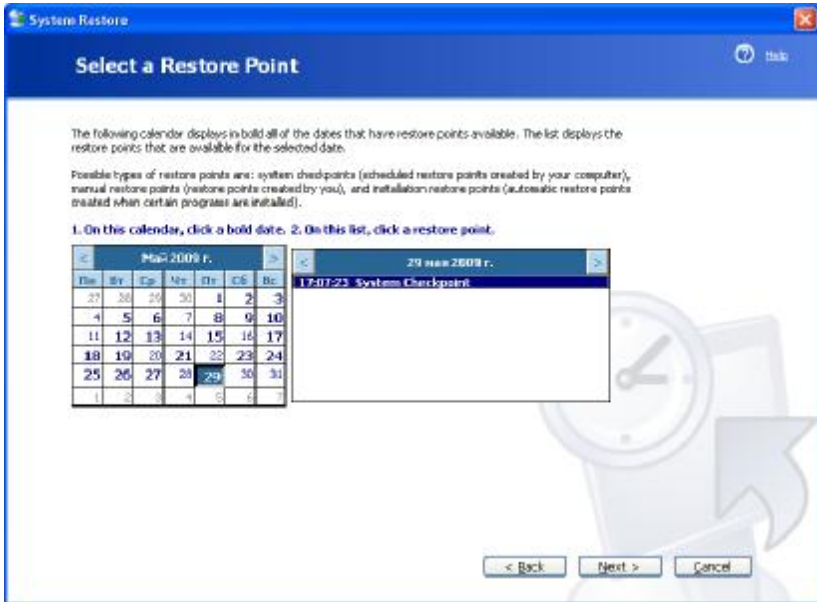
- დაბრუნების წერტილი იქმნება ყოველთვის, როცა ხდება Windows-ის განახლება უტილიტებით Windows Update ან Automatic Updates.

- როდესაც ვუბრუნდებით წინა კონფიგურაციას System Restore-ის საშუალებით, ხდება მიმდინარე კონფიგურაციის დამახსოვრება. აუცილებლობის შემთხვევაში შეგიძლიათ გააუქმოთ აღდგენა.

- როდესაც ახლენთ ფაილების აღდგენას Windows Backup-ის საშუალებით, System Restore უტილიტა შექმნის დაბრუნების წერტილს. თუ ფაილების აღდგენა გამოიწვევს პრობლემებს სისტემურ

ფაილებთან დაკავშირებით, თქვენ შეგიძლიათ დაუბრუნდეთ შრომისუნარიან კონფიგურაციას.

არსებობს საშუალება, შექმნათ საკუთარი დაბრუნების წერტილი. ამისათვის აირჩიეთ ბრძანება Start→All Programs→Accessories→System Tools→System Restore. ეკრანზე გამოსულ დიალოგურ ფანჯარაში აირჩიეთ ბრძანება Create A Restore Point დააჭირეთ ღილაკს Next . იხილეთ ნახ.5.5.



ნახ.5.5

System Restore სამსახური არ ახდენს დოკუმენტების, ფაილების, ელექტრონული ფოსტის ან სხვა რომელიმე ფაილების ასლების შექმნას, რომლებიც ინახება საქალაქებში My Documents, Favorites, Cookies, Recycle Bin, Temporary Internet Files, History ან Temp.

ამისათვის, რომ აღადგინოთ სისტემა წინა კონფიგურაციით დარეგისტრირდეთ Administrators ვეგუვის აღრიცხვის ჩანაწერით, გააქტიურეთ System Restore უტილიტა და აირჩიეთ ოფცია Restore My Computer To An Earlier Time (აღდგეს კომპიუტერის თავდაპირველი მდგომარეობა), დააჭირეთ ღილაკს Next და აირჩიეთ სათანადო თარიღი.

სისტემის აღდგენა ASR დისკის საშუალებით.

Automated System Recovery (ASR) დისკი – ესაა Windows XP Professional-ის შესაძლებლობა, რომლის დანიშნულებაცაა აღადგინოს სისტემა მოულოდნელი და სრული დაზიანების დროს. სისტემის სრული აღდგენა შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ ASR-დისკს თან ახლავს სისტემის სარეზერვო ასლი, შექმნილი Windows Backup-ის მიერ. ASR-ის სარეზერვო ნაკრები შეიცავს სისტემური ტომის მთელ შემცველობას, დისკების ტომების სისტემური ფაილებისა და ინსტალირებული აპარატურული უზრუნველყოფის მიმდინარე კონფიგურაციის შესახებ ინფორმაციას.

ყურადღება: თუ შექმნით ASR-ნაკრებს, Windows Backup-ის Advanced Mode რეჟიმში, მოხდება მხოლოდ სისტემური ტომის სარეზერვო ასლის შექმნა. თუ გინდათ სარეზერვო ასლში ჩართოდ სხვა დისკები, გამოიყენეთ ოსტატი Backup And Restore wizard, და აირჩიეთ ოფცია All Information On This Computer. შედეგად მოხდება ყველა დისკის სარეზერვო ასლის შექმნა.

5.3.უსაფრთხოების მდგომარეობის შემოწმება MBSA უტალიტით.

Windows Update უტილიტის საშუალებით ძნელია თვალის დევნება ყველა იმ ახალ შესწორებასა და განახლებაზე, რომელიც Windows-ისათვისაა განკუთვნილი. უტილიტა Microsoft Baseline Security Analyzer (MBSA)-ს აქვს ახალი შესწორებების მხარდაჭერა, და ამავე დროს ადარებს მათ იმ პარამეტრებთან, რომლებიც დაყენებულია ერთ ან რამოდენიმე კომპიუტერზე. MBSA ამოწმებს კომპიუტერებს საყოველთაოდ ცნობილი სუსტი ადგილების არსებობაზე (მაგალითად, მოკლე პაროლები ან უსაფრთხოების სისტემის არასწორი კონფიგურაცია) შემდეგ პროგრამულ საშუალებებს: Windows, Internet Information Services, Microsoft SQL Server და Office-ის ოჯახის პროდუქტებს.

MBSA შეგიძლიათ გამოიყენოთ საკუთარი კომპიუტერის ან ქსელში ჩართული კომპიუტერების შესამოწმებლად. MBSA-ს შესახებ ინფორმაციის მისაღებად შეგიძლიათ მიმართოთ სტატიას Q320445

Microsoft Knowledge Base. ამ სტატიაში ნახავთ მიმართვას ფაილზე (mbsasetup.msi), საიდანაც შეძლებთ MBSA უტილიტის ინსტალაციას.

უტილიტით სარგებლობისათვის აუცილებელია იქონიოთ ადმინისტრატორის უფლებები. MBSA-ს გააქტიურების შემდეგ ეკრანზე გამოჩნდება ნახ.5.6-ზე ნაჩვენები ფანჯარა.

აირჩიეთ თქვენთვის საჭირო ფუნქცია. შემდეგ ეტაპზე შეგიძლიათ აირჩიოთ ქვემოჩამოთვლილი შესასრულებელი ტესტები:

– Check for Windows vulnerabilities. ეს ოფცია ამოწმებს სისტემას არაუსაფრთხო გამართვაზე. მაგალითად, უტილიტას შეუძლია შეამოწმოს დაფორმატებულია თუ არა ყველა დისკი NTFS ფაილური სისტემის გამოყენებით.

– Check for weak passwords. მოწმდება პაროლები თითოეული აღრიცხვის ჩანაწერისათვის და იმ შემთხვევაში თუ პაროლი არ არსებობს ან არ პასუხობს უსაფრთხოების მოთხოვნებს, გაიცემა შესაბამისი შეტყობინება.

– Check for IIS vulnerabilities. ეს ოფცია ამოწმებს Internet Information Services სისტემას არაუსაფრთხო გამართვაზე. იმ შემთხვევაში, თუ IIS პაკეტი არ არის ინსტალირებული, გაიცემა შესაბამისი შეტყობინება.

– Check for SQL vulnerabilities. ეს ოფცია ამოწმებს SQL Server-ს არაუსაფრთხო გამართვაზე. თუ SQL Server-ი არ არის ინსტალირებული, გაიცემა შესაბამისი შეტყობინება.

– Check for hotfixes. ამ ოფციის არჩევისას MBSA-ა ჩატვირთავს უკანასკნელ ინფორმაციას და შეამოწმებს მითითებულ კომპიუტერებს კრიტიკული განახლებების არსებობაზე.

ნახ.5.7-ზე მოცემულია MBSA-ს შემოწმების შედეგები.

- წითელი კრიტიკულად სუსტ ადგილებს;
- ყვითელი ჯვარი გვიჩვენებს, რომ კომპიუტერმა ვერ გაიარა ტესტი განახლებებზე;
- მწვანე ალამი გვიჩვენებს, რომ ყველაფერი წესრიგშია.



636.5.6

Sort Order: ▼

Security Update Scan Results

Score	Issue	Result
	Office Security Updates	35 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
	Windows Security Updates	51 security updates are missing. 5 service packs or update rollups are missing. What was scanned Result details How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	Updates are not automatically downloaded or installed on this computer. What was scanned How to correct this
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details

636.5.7

თავი 6. მოვლენათა მონიტორინგი უსაფრთხოების სისტემაში

6.1. მოვლენათა აუდიტი

კომპიუტერის მდგომარეობაზე მუდმივად თვალყურის დევნება საკმაოდ რთულია. ბუნებრივია, ეს პროცესი უფრო რთულდება, როდესაც საჭიროა ქსელში ჩართული რამოდენიმე კომპიუტერის კონტროლი.

Windows XP Professional-ს აქვს საშუალება შეამოწმოს სისტემის უსაფრთხოებაში არსებული “სუსტი ადგილები”, ახდენს რა მოვლენათა რეგისტრაციას სპეციალურ ჟურნალებში. ეს ჟურნალებია: უსაფრთხოების ჟურნალი (Security log), დანართების ჟურნალი (Application log) და სისტემური ჟურნალი (System log). აუდიტის პროცესში უსაფრთხოების ჟურნალში აღირიცხება მომხმარებელთა მიერ შესრულებული მოვლენები.

უსაფრთხოების აუდიტის ჩართვა ხდება შემდეგი ბრძანებებით:

1. Control Panel → Administrative Tools → Local Security Policy
ან ბრძანებათა სტრიქონში აკრიფეთ secpol.msc;
2. აირჩიეთ ბრძანება Security Settings → Local Policies → Audit Policy;
3. თავუს მარცხენა ღილაკზე ორჯერ დაჭერით შეგიძლიათ აირჩიოთ ის პოლიტიკა, რომლისთვისაც გსურთ უსაფრთხოების აუდიტის დანიშვნა. აირჩიეთ ალამი Success (წარმატება), Failure (წარუმატებლობა) ან ორივე ერთად.

ცხრილში განხილულია უსაფრთხოებასთან დაკავშირებული აუდიტის პოლიტიკები.

აღრიცხვის ჩანაწერების რეგისტრაციის მოვლენათა აუდიტი	ეს მოვლენა წარმოიშობა მაშინ, როდესაც მომხმარებელი ცდილობს რეგისტრაცია გაიაროს (ან უარი თქვას რეგისტრაციაზე) ქსელში, ამასთან ხდება მომხმარებლის სააღრიცხვო ჩანაწერის იდენტიფიკაცია.
აღრიცხვის ჩანაწერების მართვის აუდიტი	აღრიცხვის ჩანაწერების მართვასთან დაკავშირებული მოვლენები წარმოიშობა მომხმარებელთა აღრიცხვის ჩანაწერების

	<p>ან უსაფრთხოების ჯგუფების შექმნის, შეცვლის ან წაშლის დროს; მომხმარებლის აღრიცხვის ჩანაწერის აქტივაციის, გამორთვის, სახელის გადარქმევის ან პაროლის დანიშვნის დროს.</p>
<p>კატალოგების სამსახურთან მიმართვის აუდიტი</p>	<p>კატალოგების სამსახურთან მიმართვის მოვლენები წარმოიშვება მაშინ, თუ მომხმარებელი ცდილობს მოიპოვოს მიმართვა Active Directory-სთან. (თუ კომპიუტერი არ არის ჩართული Microsoft Windows-ის დომენის შემადგენლობაში, მსგავსი ტიპის მოვლენები არ წარმოიშობა)</p>
<p>რეგისტრაციასთან დაკავშირებული მოვლენათა აუდიტი</p>	<p>ეს მოვლენები წარმოიშობა იმ შემთხვევაში თუ მომხმარებელი ეცდება მუშა სადგურიდან ინტერაქტიულ რეჟიმში გაიაროს რეგისტრაცია.</p>
<p>ობიექტებთან მიმართვის აუდიტი</p>	<p>ეს მოვლენები დაკავშირებულია ფაილებთან, საქაღალდეებთან, პრინტერებთან, სისტემური რეესტრის გასაღებთან ან იმ ობიექტებთან (რომლებისთვისაც ჩართულია აუდიტი) მიმართვის მცდელობის შემთხვევაში, რომელთათვისაც არჩეულია აუდიტი.</p>
<p>პოლიტიკის შეცვლის აუდიტი</p>	<p>ეს მოვლენა წარმოიშობა მაშინ, თუ მოხდა მომხმარებელთა მიმართვის უფლებების, აუდიტის, პაროლების დანიშვნის პოლიტიკის შეცვლა.</p>
<p>პრივილეგიების გამოყენების აუდიტი</p>	<p>ეს მოვლენა წარმოიშობა მაშინ, თუ მომხმარებელი გამოიყენებს ისეთ მიმართვის წესებს, რომლებიც განსხვავდება შემდეგი მიმართვებისაგან: რეგისტრაცია, სისტემიდან გასვლა ან ქსელთან მიმართვა.</p>

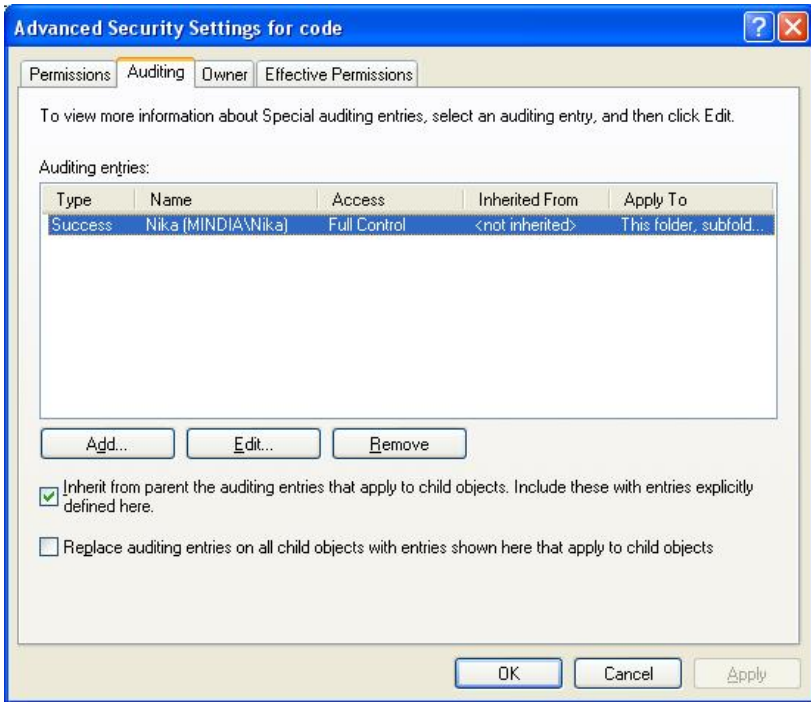
<p>პროცესებზე თვალყურის დევნების აუდიტი</p>	<p>ამ კატეგორიაში ხვდება ისეთი მოვლენები, როგორებიცაა პროგრამის აქტივიზაცია, დესკრიპტორის დუბლირება, ობიექტთან არაპირდაპირი მიმართვა და პროცესიდან გასვლა. მართალია, ეს პოლიტიკა ახდენს დიდი რაოდენობით პოლიტიკების გენერაციას, ამ დროს შეიძლება სასარგებლო ინფორმაციის დაფიქსირება, მაგალითად ცნობები იმ პროგრამის მომხმარებელზე, რომლებმაც მიიღეს ობიექტთან მიმართვის უფლება.</p>
<p>სისტემურ მოვლენათა აუდიტი</p>	<p>სისტემური მოვლენები წარმოიშობა მაშინ, თუ მომხმარებელი გადატვირთავს ან გამორთავს კომპიუტერს, ასევე თუ მოვლენა გავლენას ახდენს სისტემის უსაფრთხოებაზე ან რეგისტრაციას გადის უსაფრთხოების ჟურნალში.</p>

6.2. ფაილებთან და პრინტერებთან მიმართვის უსაფრთხოების აუდიტის კონფიგურირება

MsWindows ოპერაციულ სისტემას შეუძლია აკონტროლოს სისტემურ და სამომხმარებლო მოვლენათა მთელი რიგი. კონკრეტული ობიექტისათვის უსაფრთხოების აუდიტის ჩასართავად, აუცილებელია იქონიო ადმინისტრატორის უფლებები და შეასრულოთ შემდეგი მოქმედებები:

1. ჩართეთ უსაფრთხოების აუდიტი Local Security Settings. გააქტიურეთ Audit object access (ობიექტებთან მიმართვის აუდიტის პოლიტიკა).

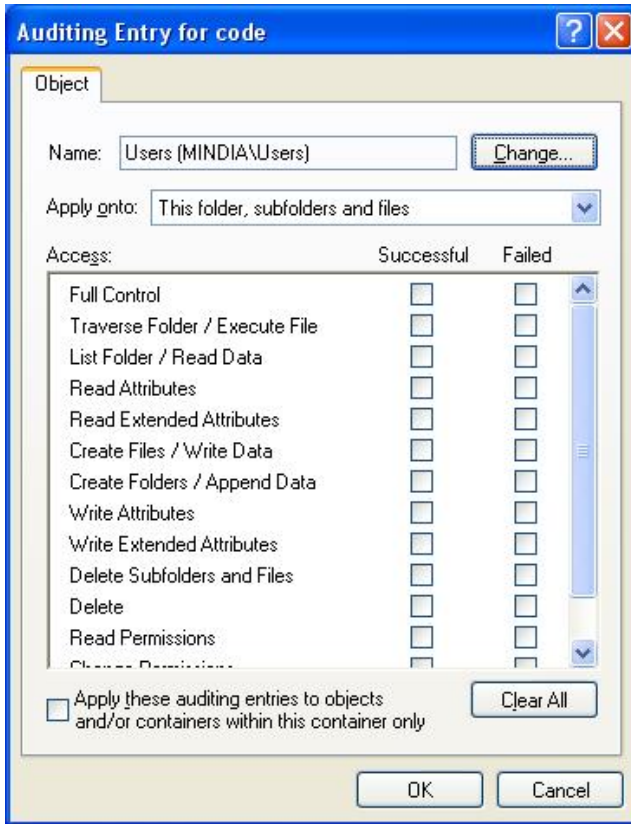
2. My computer საქალაქში აირჩიეთ საჭირო ობიექტი და მისი (ფაილის, საქალაქის, პრინტერის) თვისებები (Properties). დააჭირეთ ლილაკებზე Security, Advanced და Auditing. იხილეთ ნახ.6.1.



ნახ.6.1

3. დაჭირეთ ღილაკზე Add, აირჩიეთ აღრიცხვის ჩანაწერის ან უსაფრთხოების ჯგუფის დასახელება.

4. დიალოგურ ფანჯარაში Auditing Entry აირჩიეთ ის მიმართვის უფლებები, რომელთა გაკონტროლებაცაა საჭირო ამორჩიული აღრიცხვის ჩანაწერისა თუ უსაფრთხოების ჯგუფისათვის. ნახ.6.2-ზე და ნახ.6.3-ზე ნაჩვენებია ოფციები სვადანსვა ტიპის ობიექტებისათვის. თუ არჩეულია ალამი Successful (წარმატებული) , უსაფრთხოების ჟურნალში ჩაიწერება ჩანაწერი, რომელიც შეიცავს მომხმარებლის (ჯგუფის) მიერ მითითებული ფაილის ან საქალაღის წარმატებულად გამოყენების საათსა და თარიღს. ანალოგიურად, თუ ჩართულია ალამი Failed (წარუმატებელი), უსაფრთხოების ჟურნალში ჩანაწერი ჩაიწერება ყოველთვის, როდესაც მითითებულ ფაილთან ან საქალაღდესთან მიმართვის მცდელობა იქნება წარუმატებელი.



ნახ.6.2

ქვემოთ ჩამოთვლილია რჩევები უსაფრთხოების აუდიტის გამოყენებასთან დაკავშირებით:

- არ გამოიყენოთ უსაფრთხოების აუდიტი, თუ ამის საჭიროება არ არსებობს. აუცილებელია ზუსტად ამოიჩინოთ შესამოწმებელი მოვლენები. უსაფრთხოების ჟურნალის ზომა ფიქსირებულია და მისი შევსება უმნიშვნელო მოვლენებით არ ღირს, რათა არ მოხდეს მნიშვნელოვანი მოვლენების გამოდევნება;

- აკონტროლოთ სისტემაში რეგისტრაციის წარუმატებელი (Failure) მცდელობები, რომლებიც მიუთითებენ იმაზე, რომ ვიღაც ცდილობდა გამოეყენებინა არასწორი პაროლები;

- თუ ეჭვობთ, რომ ვიღაც ეცდება სისტემაში დარეგისტრირდეს მოპარული პაროლით, აკონტროლეთ სისტემაში რეგისტრაციის წარმატებული (Success) მცდელობები;

- არაავტორიზებული მომხმარებლის მიერ მნიშვნელოვანი ფაილების გამოყენების აღმოსაჩენად, აკონტროლეთ წარმატებული მიმართვა კითხვისა და ჩაწერის რეჟიმზე ამ ფაილებისათვის;

- ვირუსული პროგრამების აღმოსაჩენად, აკონტროლეთ წარმატებული მიმართვა ჩაწერის რეჟიმზე პროგრამების ფაილებისათვის (ფაილები გაფართოებით exe, com და dll);

- იმისათვის, რომ აღმოაჩინოთ, თუ ვინ ბეჭდავს ფერად კარტრიჯზე აკონტროლეთ წარმატებული მიმართვა პრინტერის გამოყენებაზე.



ნახ.6.3.

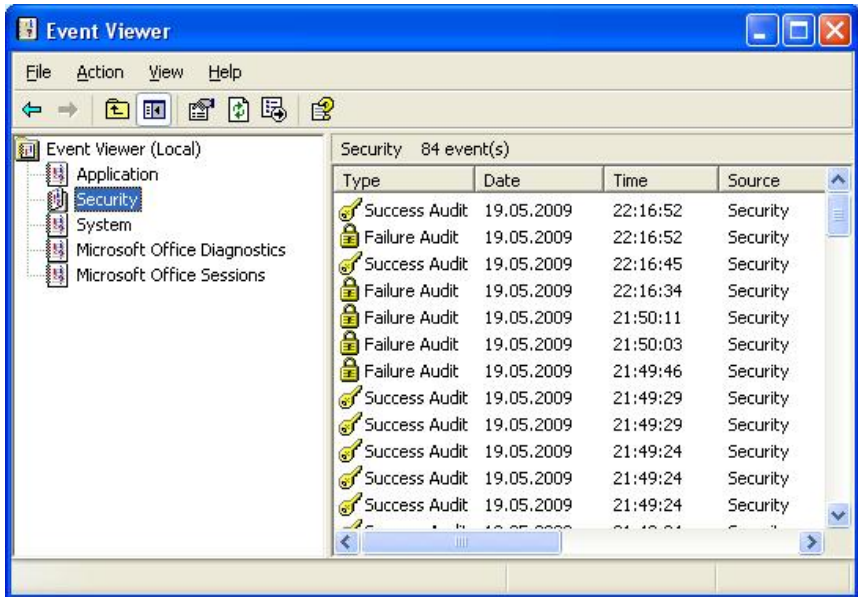
6.3. უსაფრთხოების ჟურნალის დათვალიერება

უსაფრთხოების ჟურნალის დასათვალიერებლად გამოიყენება Event Viewer უტილიტა. მის გასააქტიურებლად შეასრულეთ ბრძანება:


Control Panel → Administrative Tools → Event Viewer


ან ბრძანებათა სტრიქონში აკრიფეთ ბრძანება eventvwr.msc.

Event Viewer-ის საშუალებით შესაძლებელია სამივე ჟურნალის დათვალიერება. ესენია: დანართების ჟურნალი (Appevent.evtx), უსაფრთხოების ჟურნალი (Secevent.evtx) და სისტემური ჟურნალი (Sysevent.evtx). იხილეთ ნახ.6.4.



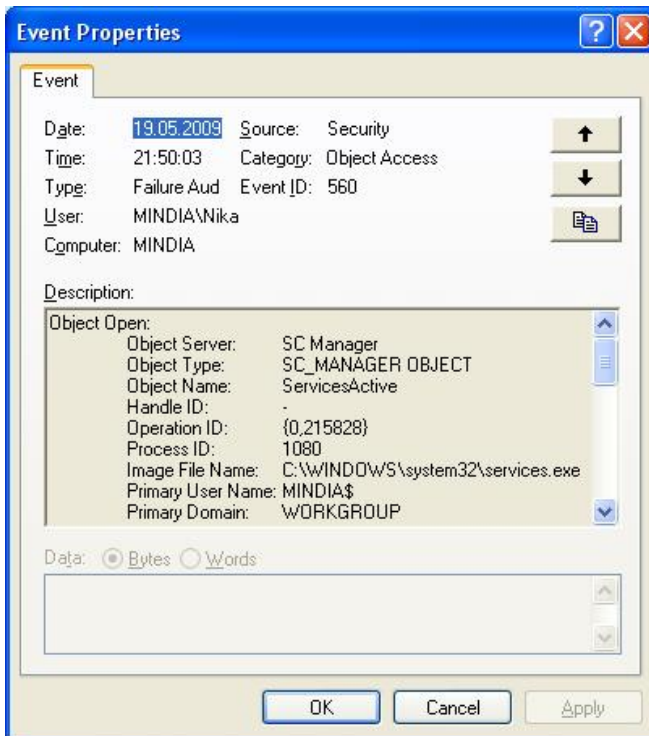
ნახ.6.4

 — მიუთითებს შესამოწმებელი მოვლენის წარმატებით დასრულებაზე.

 — მიუთითებს შესამოწმებელი მოვლენის წარუმატებლად დასრულებაზე.

გაჩუქების პრინციპით დანართების ჟურნალი და სისტემური ჟურნალი შეუძლიათ დაათვალიერონ Everyone ჯგუფის წევრებმა, ხოლო უსაფრთხოების ჟურნალის დაათვალიერება შეუძლიათ მხოლოდ Administrators ჯგუფის წევრებს და ასევე მხოლოდ ამ უკანასკნელი ჯგუფის წევრებს შეუძლიათ ამ სამივე ჟურნალის გასუფთავება.

მოვლენის შესახებ დამატებითი ინფორმაციის მისაღებად, აირჩიეთ საჭირო მოვლენა, დააჭირეთ 2-ჯერ თავუს მარცხენა ღილაკს, ეკრანზე გაიხსნება Event Properties ფანჯარა იხილეთ ნახ.6.5.

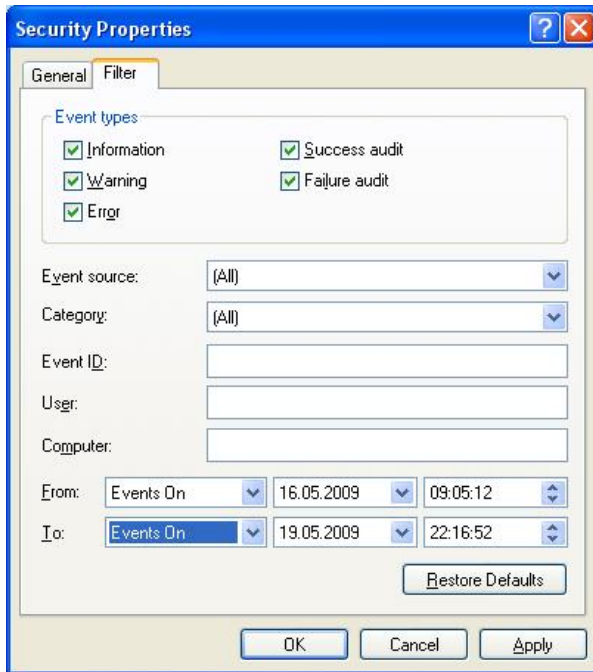


ნახ6.5

რომელიმე კონკრეტული მოვლენის მოძებნა შეიძლება ბრძანებით View→Find.

ჟურნალში მოთავსებული მოვლენები შეგიძლიათ გაფილტროთ ბრძანებით View→Filter. მაგალითად, გვიანტერესებს მოვლენები,

რომელთაც ადგილი ჰქონდათ დროის განსაზღვრულ ინტერვალში.
იხილეთ ნახ.6.6.



ნახ.6.6

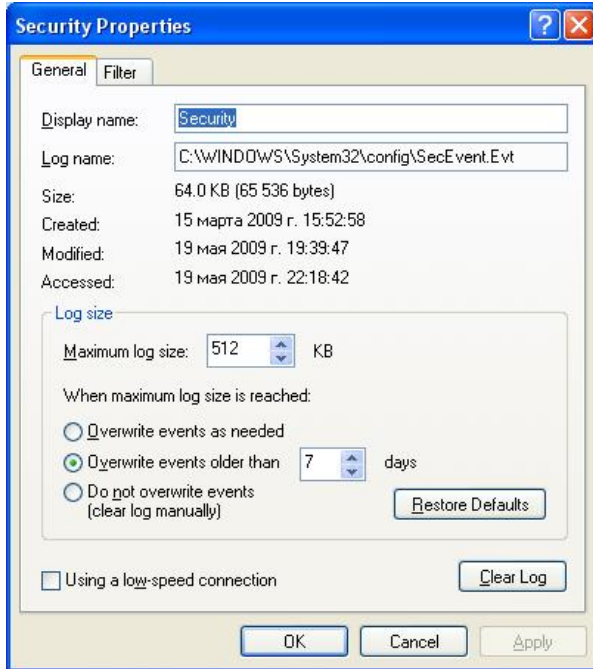
6.4. ჟურნალების ფაილების დამუშავება

გაჩუმების პრინციპით, სამივე ჟურნალის საერთო ზომა არ უნდა აღემატებოდეს 512 კბაიტს. დასაშვებია მისი შემცირება ან გაზრდა. თითოეულ ჟურნალში მოვლენები ინახება 7 დღე, თუმცა შეიძლება ამ პარამეტრის შეცვლაც. იხილეთ ნახ.6.7.

ჟურნალის არქივის შესაქმნელად აირჩიეთ ბრძანება:

View → Save Log File As

ეკრანზე გამოსულ დიალოგურ ფანჯარაში აირჩიეთ ფაილის ტიპი Event Log (*.evt), რის შედეგადაც მიიღება ჟურნალის სრული ასლი, რომლის დათვალიერებაც შეიძლება მხოლოდ Event Viewer უტილიტით.



ნახ.6.7

საკონტროლო კითხვები:

1. როგორ მოვახდინოთ ფაილის კოდირება/დეკოდირება?
2. როგორ აღვადგინოთ დაზიანებული სექტორები დისკზე?
3. რის საშუალებას იძლევა უტილიტა MBSA?
4. როგორ შევქმნათ მონაცემების სარეზერვო ასლები?
5. როგორ ჩავრთოთ უსაფრთხოების აუდიტი?
6. როგორ ჩავრთოთ საქალაქდესთან მიმართვის მოვლენათა აუდიტი?
7. როგორ დავათვალიეროთ უსაფრთხოების ჟურნალი?

თხზი.7. ჯგუფური პოლიტიკები.

7.1.უსაფრთხოების უზრუნველყოფასთან დაკავშირებული პოლიტიკები

ჯგუფური პოლიტიკა – ესაა Ms Windows XP-ის ფუნქცია, რომელიც საშუალებას აძლევს ადმინისტრატორს მოახდინოს კომპიუტერის კონფიგურაციის პარამეტრების დაყენება, და ამავე დროს არ აძლევს უფლებას მომხმარებელს შეცვალოს უკვე დადგენილი კონფიგურაცია.

ჯგუფური პოლიტიკის საშუალებით შესაძლებელია უსაფრთხოების პოლიტიკების მართვა. უსაფრთხოების პოლიტიკების დათვალიერება შეიძლება ორი გზით:

1. აირჩიეთ ბრძანება Administrative Tools → Local Security Policy ან ბრძანებათა სტრიქონში აკრიფეთ Secpol.msc. იხილეთ ნახ.7.1.



ნახ.7.1

7.2. მომხმარებლის მიმართვის უფლება

ტერმინი “მომხმარებლის მიმართვის უფლება” იგულისხმება პოლიტიკების ნაკრები, რომლებიც განსაზღვრავენ იმ მოქმედებებს, რომელთა შესრულების უფლებაც უსაფრთხოების ჯგუფებში შემავალ მომხმარებლებს ეძლევათ. ACL-ისაგან განსხვავებით, რომელიც კონკრეტულ ობიექტებთან (ფაილები ან პრინტერი) მიმართვას აკონტროლებს, მომხმარებლის მიმართვის უფლება ისეთი ოპერაციების შესრულებას ეხება, რომლებიც მთლიანად კომპიუტერზე მოქმედებენ.



ნახ.7.2

მომხმარებლის მიმართვის უფლება მოიცავს უფლებათა ორ ფართო კატეგორიას: რეგისტრაციის უფლებები და პრივილეგიები. რეგისტრაციის წესები განსაზღვრავენ მათ, ვისაც აქვთ კომპიუტერთან მიმართვის უფლება. პრივილეგიები კი განსაზღვრავენ იმ

მომხმარებლებს, რომელთაც კომპიუტერზე განსაზღვრული მოქმედებების შესრულების უფლება აქვთ. მაგალითად, ფაილების სარეზერვო კოპირება.

თითოეული მომხმარებლის აღრიცხვის ჩანაწერის ან მომხმარებელთა ჯგუფებში ცვლილებების სანახავად აირჩიეთ ბრძანება:

Security Settings → Local Policies → User Rights Assignment

იმ მომხმარებელთა აღრიცხვის ჩანაწერების და უსაფრთხოების ჯგუფების სიის შესაცვლელად, რომელთაც დანიშნული აქვთ კონკრეტული მიმართვის უფლებები, საჭიროა:

1. აირჩიეთ უფლება თავუს მარცხენა ღილაკის 2-ჯერ დაჭერით.
2. ეკრანზე გამოჩნდება თვისებათა დიალოგური ფანჯარა, სადაც Add ღილაკით შეგიძლიათ დაამატოთ საჭირო მომხმარებლის აღრიცხვის ჩანაწერი ან უსაფრთხოების ჯგუფი. (იხილეთ ნახ. 7.2.)

7.3. უსაფრთხოების უზრუნველყოფის პარამეტრები

უსაფრთხოების პარამეტრების პოლიტიკებს აქვთ მრავალი საინტერესო ოფცია, რომლებიც განსაზღვრავენ სისტემის მოქმედებას. აირჩიეთ ბრძანება Security Settings→Local Policies→Security Options.

ამ პოლიტიკების “გაჩუმების პრინციპით” დანიშნული პარამეტრები უზრუნველყოფენ უსაფრთხოების სავსებით დამაკმაყოფილებელ დონეს, რომელიც მისაღებია მომხმარებელთა უმრავლესობისათვის. თუ გადაწყვიტავთ ცვლილებების შეტანას, თავდაპირველად აუცილებელია დაკვირვებით გაეცნოთ პოლიტიკის აღწერას და მერე შეცვალოთ. ზოგიერთი პოლიტიკისათვის მდგომარეობა Enabled (ჩართული) წარმოადგენს უფრო უსაფრთხოს, ხოლო სხვა შემთხვევაში უმჯობესია გამოიყენოთ Disabled (გამორთული).

ცხრილში აღწერილია უსაფრთხოების პოლიტიკების ის პარამეტრები, რომლებიც უზრუნველყოფენ სისტემის უსაფრთხო ფუნქციონირებას ლოკალური კომპიუტერების შემთხვევაში. დანარჩენი პოლიტიკები (აქ არ განიხილება) გამოიყენება, როგორც წესი, დიდი ღომენების შემადგენლობაში შემავალი კომპიუტერებისათვის.

Accounts: Administrator account status	ეს პოლიტიკა Disabled მდგომარეობაში ბლოკავს Administrator-ის აღრიცხვის ჩანაწერს. ბლოკირების შემთხვევაში აღრიცხვის ჩანაწერი მიღწევადია Safe Mode რეჟიმში.
Accounts: Guest account status	ეს პოლიტიკა Disabled მდგომარეობაში ბლოკავს Guest-ის აღრიცხვის ჩანაწერს.
Accounts: Limit local account use of blank passwords to console logon only	ეს პოლიტიკა ჩართულია გაჩუმების პრინციპით. ხელს უშლის მომხმარებელთა დაშორებულ რეგისტრაციას ისეთი მომხმარებლის აღრიცხვის ჩანაწერით, რომელსაც არ აქვს პაროლი. სისტემის უსაფრთხო ფუნქციონირების უზრუნველყოფის მიზნით, ყოველთვის სასურველია ჩართული იყოს ეს პოლიტიკა.
Accounts: Rename administrator account	ამ პოლიტიკის საშუალებით შესაძლებელია ადმინისტრატორის აღრიცხვის ჩანაწერის შესაბამის SID იდენტიფიკატორს მიენიჭოს სხვა სახელი. ამ მიდგომის გამოყენება მოსახერხებელია ჰაკერებისაგან Administrator-ის აღრიცხვის ჩანაწერს დამალვის მიზნით.
Accounts:Rename guest account	ამ პოლიტიკის საშუალებით შესაძლებელია Guest აღრიცხვის ჩანაწერის შესაბამისი SID იდენტიფიკატორის სახელის შეცვლა. ეს დამალული პოტენციური “შესვლის” წერტილი ცნობილია ყველა ბოროტმოქმედისათვის.
Audit: Audit the access of global system objects	ეს პოლიტიკა საშუალებას იძლევა შეასრულოთ სხვა დამატებითი სისტემური ობიექტების აუდიტი, იმ შემთხვევაში, თუ არჩეულია ობიექტებთან მიმართვის აუდიტი. ეს პოლიტიკა გაჩუმების პრინციპით ბლოკირებულია, მისი შართვა ხდება განსაკუთრებულ შემთხვევებში.
Audit: Audit the use of Backup and	ჩვეულებრივ, როდესაც ხდება ფაილების სარეზერვო კოპირება ან აღდგენა, უსაფრთხოების უზრუნველყოფის მიზნით ჩანაწერები არ იწერება, აუდიტის

Restore privilege	პრივილეგიების ჩართვის შემთხვევაშიც კი. ამ პოლიტიკის გააქტიურებისას განიხილება პრივილეგიის თითოეული გამოყენება.
Audit: Shut down system immediately if unable to log security audits	იმის და მიხედვით, თუ როგორაა კონფიგურირებული მოვლენათა რეგისტრაციის პარამეტრები, უსაფრთხოების ჟურნალი შესაძლოა გადაივსოს და შეუძლებელი გახდეს მასში დამატებითი ჩანაწერების შეტანა. ამის გამო უსაფრთხოების ჟურნალი ვეღარ აფიქსირებს მოვლენებს. ამ პოლიტიკის გააქტიურება, ასეთ შემთხვევაში გათიშავს კომპიუტერს. მუშა მდგომარეობის აღსადგენად, ადმინისტრატორმა უნდა გაწმინდოს უსაფრთხოების ჟურნალი და შემდეგ თავიდან დააყენოს სისტემური რეგისტრის მნიშვნელობები.
Interactive logon: Do not display last user name	თუ ეს პოლიტიკა დაბლოკილია (გაჩუმების პრინციპით), დიალოგური ფანჯარა Log On To Windows ასახავს ბოლოს დარეგისტრირებული მომხმარებლის სახელს. პოლიტიკის გააქტიურების შემთხვევაში ველი User Name რჩება ცარიელი.
Interactive logon: Do not require Ctrl+Alt+Del	თუ ეს პოლიტიკა გათიშულია, მომხმარებელმა უნდა აკრიფოს Ctrl+Alt+Del კლავიშების კომბინაცია Log On To Windows დიალოგური ფანჯრის გამოსატანად. ეს პოლიტიკა არ იძლევა ეფექტს, თუ კომპიუტერი კონფიგურირებულია Welcome ეკრანის გამოტანის გათვალისწინებით.
Interactive logon: Message text for users attempting to log on	ეს პოლიტიკა განსაზღვრავს იმ შეტყობინების ტექსტს, რომელიც გამოიტანება თითოეული რეგისტრაციის წინ. (იხ.თავი2)
Interactive logon: Message title for users attempting to log on	ეს პოლიტიკა განსაზღვრავს იმ შეტყობინების ტექსტის სათაურს, რომელიც გამოიტანება თითოეული რეგისტრაციის წინ. (იხ.თავი2)
Interactive logon: Prompt user to	ეს პოლიტიკა მიუთითებს იმ დღეების რაოდენობას, რომელთა გასვლის შემდეგაც

change passwords before expiration	მომხმარებლის აღრიცხვის ჩანაწერი წყვეტს ფუნქციონირებას.
Interactive logon: Smart card removal behavior	ეს პოლიტიკა მიუთითებს, თუ რა მოხდება, თუ რეგისტრირებული მომხმარებლის სმარტ-ბარათი ამოიღეს სმარტ-ბარათის ჩასადებიდან. (სმარტ-ბარათი წარმოადგენს საკრედიტო ბარათის ზომის მოწყობილობას, სადაც ინახება მონაცემები სერთიფიკატებისა და პაროლების შესახებ. სმარტ-ბარათის მიმღებით აღჭურვილ კომპიუტერზე, რეგისტრაციისათვის მომხმარებელი პაროლს აკრების ნაცვლად, სმარტ-ბარათს ჩადგამს.) შესაძლებელია ამ პოლიტიკის ისეთი სახით დაყენება, რომ ზედმეტი პრობლემების გარეშე დაიბლოკოს მომხმარებლის რეგისტრაცია.
Shutdown: Allow system to be shut down without having to log on	გაჩუქების პრინციპით დიალოგური ფანჯარა Log On To Windows შეიცავს ღილაკს Shutdown. ამ პოლიტიკის გათიშვის შემთხვევაში ღილაკი მიუღწევადია. ასეთ შემთხვევაში მხოლოდ ის მომხმარებელი შეძლებს კომპიუტერის გათიშვას, რომელიც წარმატებით დარეგისტრირდა.
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	ამ პოლიტიკის გააქტიურების შედეგად ფაილების კოდირება/დეკოდირებისათვის კოდირების ფაილური სისტემა (EFS) გამოიყენებს 3DES სტანდარტს DESX ალგორითმის ნაცვლად. (იხილეთ თავი 3)

7.4. ჯგუფური პოლიტიკები

Windows XP-ში არსებობს ასობით ჯგუფური პოლიტიკა. უმრავლესობა მათგანი აკონტროლებს მომხმარებელთა ინტერფეისს, ასევე განსაზღვრავს იმ ფუნქციების ნაკრებს, რომელთა შესრულების უფლებაც აქვს მომხმარებელს. ნებისმიერ პოლიტიკას აქვს სამი

პარამეტრი : Not Configured - არ გამოიყენება, Enabled - ჩართულია ან Disables - გამორთულია. “გაჩუმების” პრინციპით Group Policy-ის ყველა პოლიტიკას აქვს მნიშვნელობა Not Configured.

პარამეტრების შესაცვლელად აირჩიეთ საჭირო პოლიტიკა (2-ჯერ კლიკი). დაილოგურ ფანჯარაში properties შეგიძლიათ აირჩიოთ ზემოჩამოთვლილი ოფციებიდან ერთ-ერთი, ხოლო Explain ღილაკი იძლევა დაწვრილებით ცნობებს ამა თუ იმ პოლიტიკის შესახებ. უფრო კონკრეტული ინფორმაცია თითოეული პოლიტიკის შესახებ მისაწვდომია საიტზე : <http://www.microsoft.com/windows2000/techinto/reskit/en-us/default.asp/> ღილაკებით previous setting და Next Setting შეგიძლიათ მარტივად დაბრუნდეთ თავდაპირველ პარამეტრებზე.

ცხრილში აღწერილია უსაფრთხოების მხარდამჭერი ჯგუფური პოლიტიკები

პოლიტიკა	აღწერა
Computer Configuration\Administrative Templates\Windows Components\NetMeeting	
საერთო მიმართვის გათიშვა დაშორებულ სამუშაო მაგიდასთან	ეს პოლიტიკა გათიშავს NetMeeting-ის მხოლოდ იმ თვისებას, რომელიც უზრუნველყოფს დაშორებულ სამუშაო მაგიდასთან მიმართვას. (ეს თვისება საშუალებას აძლევს დაშორებულ მომხმარებელს დაათვალიეროს და აკონტროლოს თქვენი სამუშაო მაგიდა.) თუ ხდება NetMeeting-ის გამოყენება და შეუძლებელია თქვენს სამუშაო მაგიდასთან სხვა მომხმარებლის მიმართვის უფლების შეზღუდვა ისარგებლეთ ამ პოლიტიკით.

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

უსაფრთხოების
ზონები:
კონფიგურაციის
გამოყენება მხოლოდ
მოცემული
კომპიუტერისათვის

პოლიტიკა განსაზღვრავს ერთი კომპიუტერის სხვადასხვა მომხმარებლის მიერ Microsoft Internet Explorer-ის ერთი და იგივე უსაფრთხოების ზონების გამოყენებას. თუ ეს პოლიტიკა არ არის გააქტიურებული, თითოეულ მომხმარებელს დამოუკიდებლად შეუძლია მოახდინოს უსაფრთხოების ზონების კონფიგურაციის დაყენება. ამ პოლიტიკის გააქტიურება გარანტიას იძლევა, რომ თქვენს მიერ დაწესებული უსაფრთხოების ზონების მკაცრ კონფიგურაციას ერთნაირად გამოიყენებს ყველა მომხმარებელი.

უსაფრთხოების
ზონები:
მომხმარებლებს არ
აქვთ უფლება
შეცვალონ
პოლიტიკები

ეს პოლიტიკა აძლიერებს წინა პოლიტიკის მოქმედებას. მისი გააქტივირების შემთხვევაში გაითიშება დილაკები Custom Level და უსაფრთხოების დონის მარეგულირებელი Security ჩანართში, რომლებიც მდებარეობენ Internet Options დიალოგურ ფანჯარაში. ამ პოლიტიკის გააქტიურების შედეგად მომხმარებელი ვერ შეცვლის უსაფრთხოების ზონების კონფიგურაციებს.

Internet Explorer-ის
კომპონენტების
ავტომატური
ჩართვის გაითიშვა.

Web-კვანძთან მიმართვის დროს, დიალოგური ფანჯარა Security Warning ეკითხება მომხმარებელს დააყენოს თუ არა მოცემული კომპონენტი. თუ საჭიროა აუკრძალოთ მომხმარებლებს ისეთი კომპონენტების გააქტურება, რომლებიც ხელს უშლიან მუშაობის პროცესს, გამორთეთ შესაბამისი ოფცია ამ პოლიტიკის ამორჩევის გზით.

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security	
კლიენტის მიერთებისათვის კოდირების დონის მომზადება	თუ კომპიუტერზე ინსტალირებულია ოპერაციული სისტემა Windows XP და გამოიყენება დაშორებული სამუშაო მაგიდა (Remote Desktop), ხოლო დანარჩენ მასთან დაკავშირებულ კომპიუტერებზე ასევე სრულდება Windows XP, გააქტიურეთ ეს პოლიტიკა და მიანიჭეთ მნიშვნელობა High Level.
Computer Configuration\Administrative Templates\Network\Offline Files	
ქეშ-მეხსიერების შემცველობის კოდირება, რომელიც მოიცავს ავტონომიურ ფაილებსაც	ამ პოლიტიკის გააქტიურების შედეგად ხდება ავტონომიური ფაილების ყველა ლოკალური ასლის კოდირება. ამგვარად, უზრუნველყოფილია დამატებითი უსაფრთხოება იმ შემთხვევაში, თუ ჰაკერი შეძლებს თქვენს კომპიუტერთან არაკანონიერი მიმართვის უფლების მოპოვებას.
Computer Configuration\Administrative Templates\Windows Components\NetMeeting	
NetMeeting-ის უსაფრთხო გამომახების ოფციების დაყენება ავტომატური გამომახების მიღების აღკვეთა	ამ პოლიტიკის არჩევისას მოითხოვება უსაფრთხოების დაცვა ყველა შემომომავალი და გამავალი გამომახებისათვის. ეს პოლიტიკა კრძალავს NetMeeting-ის იმ თვისების გამოყენებას, რომელიც უზრუნველყოფს პასუხების ავტომატურ გენერირებას, რის შედეგადაც ნებისმიერ მომხმარებელს შეუძლია მიუერთდეს კომპიუტერს თქვენი არყოფნის პერიოდში. (ეს პოლიტიკა მოქმედებს მხოლოდ მაშინ, როდესაც გააქტიურდება NetMeeting-ი)

Computer Configuration\Administrative Templates\Windows Components\NetMeeting\Application Sharing

<p>დანართებთან საერთო მიმართვის გათიშვა</p>	<p>პოლიტიკა ბლოკავს საერთო მიმართვის შესაძლებლობას, რაც მიღწევადია NetMeeting-ის დანართების შესრულებისას. თუ ეს პოლიტიკა გააქტიურებულია მომხმარებლებს არ შეუძლიათ ერთდროულად გამოიყენონ დანართები ან ერთდროულად მიმართონ იმ დანართებს, რომლებიც მდებარეობენ სხვა კომპიუტერზე.</p>
---	---

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

<p>სერთიფიკატების პარამეტრების შეცვლის გათიშვა</p>	<p>ეს პოლიტიკა გათიშავს Certificates დილაკს, რომელიც გამოსახულია Internet Options დიალოგური ფანჯრის Content ჩანართში, რითაც უბლოკავს მომხმარებელს სერთიფიკატების დამატების ან წაშლის საშუალებას.</p>
<p>არ გამოიყენოთ ავტოშეცვლის თვისება პაროლების შენახვისათვის</p>	<p>ამ პოლიტიკის გააქტიურებისას, Internet Explorer-ი არ დაიმსხოვრებს თქვენს მიერ ვებ-გვერდებზე აკრებილ პაროლებს. გაითიშება AutoComplete Settings დიალოგური ფანჯრის ოფციები. Internet Explorer-ის საშუალებით პაროლების შენახვა რისკთან არის დაკავშირებული, რადგან უცხო პირს, რომელსაც აქვს თქვენს კომპიუტერთან მიმართვის უფლება, შეუძლია მიმართოს თქვენი პაროლებით დაცულ ვებ-საიტებს.</p>

User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel	
Security გვერდის გათიშვა	ამ პოლიტიკის გააქტიურების შედეგად დაიმალება Internet Options დიალოგური ფანჯრის ჩანართი Security, რის შედეგადაც მომხმარებლები არ დაიშვებიან უსაფრთხოების ზონების დასათვალიერებლად ან შესაცვლელად.
User Configuration\Administrative Templates\Windows Components\Windows Explorer	
განსაზღვრული დისკების დამალვა My Computers ფანჯარაში	ამ პოლიტიკის გააქტიურების შედეგად განსაზღვრული დისკები აღარ აისახება My Computers, Windows Explorer და საერთო დიალოგურ ფანჯრებში (მაგ., ფანჯარაში Open). ეს დისკები რჩება მისაწვდომი პროგრამებისათვის, ბრძანებათა სტრიქონში და სხვა არაცხადი საშუალებების გამოყენებისას.
My Computers-ის დისკებთან მიმართვის ბლოკირება	ამ პოლიტიკის საშუალებით იზღუდება ცალკეულ დისკებთან მიმართვა Windows Explorer-ის ან სხვა ინსტუმენტალური საშუალებებით. დისკები გამოჩნდებიან (თუ ისინი არ არიან დამალული წინა პოლიტიკის საშუალებით), მაგრამ მათთან მიმართვა შეუძლებელია. თუმცა, პროგრამებს შეუძლიათ მიმართონ ამ დისკებს.

<p>Security ჩანართის ამოგდება</p>	<p>ამ პოლიტიკის გააქტიურების შედეგად დაიმალება ჩანართი Security ფაილებისა და საქალაქების თვისებების დიალოგურ ფანჯარაში, რითაც ეკრძალებათ მომხმარებლებს დაათვალიერონ ან შეცვალონ მიმართვის უფლებები. გამოცდილმა მომხმარებლებმა შეიძლება აიცილონ თავიდან ეს შეზღუდვა Calcs და Xcalcs ბრძანებების გამოყენებით</p>
-----------------------------------	--

User Configuration\Administrative Templates\Windows Components\Windows Explorer\Common Open File Dialog

<p>ახლახან შექმნილი ფაილების დამალვა სიიდან</p>	<p>თუ ეს პოლიტიკა არ არის გააქტიურებული File Name ველი Open დიალოგურ ფანჯარაში შეიცავს ბოლოს გახსნილი ფაილების სიას. თუ გსურთ, რომ სხვა მომხმარებლებისათვის არ გახდეს ცნობილი ამ ფაილების დასახელებები გააქტიურეთ ეს პოლიტიკა.</p>
---	--

User Configuration\Administrative Templates\ Start Menu and Taskbar

<p>არ ინახება ჩანაწერები ბოლოს გახსნილი დოკუმენტების შესახებ.</p>	<p>როგორც წესი, თქვენს მიერ გახსნილ დოკუმენტებზე სწრაფი მიმართვა ინახება საქალაქდებში Windows, %UserProfile%\Recent. ამ პოლიტიკის გააქტიურების შედეგად წაიშლება Recent საქალაქდის შემცველობა და სხვა მომხმარებლები ვერ გაიგებენ რომელ დოკუმენტებთან მუშაობდით ბოლო დროს.</p>
---	--

<p>ბოლოს გახსნილი დოკუმენტების ჟურნალის გასუფთავება სისტემიდან გასვლის შემდეგ.</p>	<p>ამ პოლიტიკის საშუალებით სუანსის პროცესში შევიძლიათ გამოიყენოთ ბრძანება Star t→ Recent Documents და მოხერხებულად მიმართოთ იმ ფაილებს, რომლებიც ერთხელ უკვე იყო გახსნილი. ამ ფაილების სახელწოდებები სიიდან წაიშლება სისტემიდან გასვლის შემდეგ.</p>
<p>User Configuration\Administrative Templates\Control Panel</p>	
<p>Control Panel-თან მიმართვის აკრძალვა</p>	<p>ამ პოლიტიკის გააქტიურების შედეგად გაითიშება Control Panel-ი; იგი ამოვარდება Start-მენიუდან და My Computer ფანჯრიდან.</p>
<p>User Configuration\Administrative Templates\Control Panel\Display</p>	
<p>Screen Saver-ის დაცვა პაროლით</p>	<p>ამ პოლიტიკის გააქტიურების შედეგად ყველა Screen Saver-ი დაცული ხდება პაროლით.</p>
<p>User Configuration\Administrative Templates\System</p>	
<p>ბრძანებათა სტრიქონთან მიმართვის აკრძალვა</p> <p>სიტემურ რეესტრთან მიმართვის აკრძალვა რედაქტირების ინსტრუმენტების გამოყენებით.</p>	<p>ეს პოლიტიკა უკრძალავს მომხმარებლებს Cmd.exe პროგრამის გამოყენებას, საიდანაც შეიძლება ნებისმიერი პროგრამის გაშვება შესრულებაზე.</p> <p>ეს პოლიტიკა ბლოკავს რეესტრის რედაქტორს Registry Editor (Regedit.exe და Regedit32.exe).</p>

<p>მხოლოდ განსაზღვრული Windows-დანართების შესრულება</p> <p>განსაზღვრული Windows-დანართების შესრულების აკრძალვა</p>	<p>თუ ნამდვილად გინდათ თქვენი კომპიუტერის მუშაობის დაბლოკვა აირჩიეთ ეს პოლიტიკა. აქ შესაძლებელია იმ პროგრამათა სიის მითითება, რომელთა შესრულებაზე გაშვებაც შეიძლება Start-მენიუდან ან Windows Explorer-იდან.</p> <p>ამ პოლიტიკის საშუალებით შეიძლება იმ პროგრამათა სიის მითითება, რომელთა შესრულებაზე გაშვებაც არ შეიძლება.</p>
<p>User Configuration\Administrative Templates\System\Ctrl-Alt-Del Options</p>	
<p>Task Manager-ის ამოგდება</p>	<p>Ctrl-Alt-Del კლავიშების კომბინაციის საშუალებით ხდება Task Manager-ის გაშვება. ამ პოლიტიკის გააქტიურებით იბლოკება Task Manager-ი. მისი გაშვება ასევე შეუძლებელია Taskmgr.exe გამშვები ფაილითაც.</p>

7.5. სხვადასხვა მიმართვის უფლებები განსხვავებული მომხმარებლებისათვის

Group Policy-ის კონსოლის გააქტიურებისას ნათლად ჩანს, სხვადასხვა საქალაქები Computer Configuration და User Configuration. თუმცა ეს კონფიგურაციები ერთნაირად ეხება ყველა მომხმარებელს, რომელიც დარეგისტრირებულია სისტემაში. ამ მხრივ, მეტად მოქნილია Windows.Net Server, სადაც შესაძლებელია კონფიგურაციების სრული კოლექციის შექმნა სხვადასხვა კომპიუტერებისა და მომხმარებლებისათვის.

მართალია, Group Policy-ის შემთხვევაში უშუალოდ თითოეული ჯგუფისათვის კონფიგურაციის შეცვლა არ შეიძლება, შესაძლებელია გამოიყენოთ მომხმარებელთა ჯგუფი: ისინი ვისთვისაც ვრცელდება Group Policy-ში არჩეული პარამეტრები და ისინი ვისთვისაც ეს პარამეტრები არ ვრცელდება. ასეთი საშუალების მიღწევა შეიძლება User Configuration საქალაქიდან, ხოლო Computer Configuration-ში მითითებული პარამეტრები გამოიყენება სისტემაში რომელიმე მომხმარებლის რეგისტრაციამდე.

ზემოაღწერილის მიღწევა შესაძლებელია, იმ მოსაზრებიდან გამომდინარე, რომ Group Policy-ში არჩეული პოლიტიკები ვრცელდება მხოლოდ იმ მომხმარებლებზე, რომელთაც აქვთ Group Policy-ის ობიექტის წაკითხვის რეჟიმის უფლება (იგი მდებარეობს საქალაქში %SystemRoot\System32\Group Policy), ხოლო მომხმარებლებს, რომელთაც არ აქვთ წაკითხვის უფლება მათზე პოლიტიკები არ ვრცელდება. ამგვარად, თუ ავუკრძალავთ ადმინისტრატორს ან იმ მომხმარებლებს რომლებსთვისაც არ გსურთ გაავრცელოთ აკრძალვის პოლიტიკები, Group Policy საქალაქის წაკითხვის უფლებას, ისინი განთავისუფლებიან აკრძალვის პოლიტიკისაგან.

ამისათვის აირჩიეთ შემდეგი მოქმედებები:

1. შეცვალეთ ჯგუფური პოლიტიკების პარამეტრები.
2. Windows Explorer → Tools → Folder Options → View აირჩიეთ ოფცია Show Hidden Files and Folders და გამორთეთ ალამი ოფციისათვის Use Simple File Sharing;
3. აირჩიეთ საქალაქი %SystemRoot\System32\Group Policy და მისი კონტექსტური მენიუდან აირჩიეთ properties.
4. Group Policy properties დიალოგურ ფანჯარაში აირჩიეთ ოფცია Security, აირჩიეთ ჯგუფი Administrators და ჩართეთ ალამი Deny კითხვის რეჟიმზე. (შეგიძლიათ ჩაამატოთ სხვა მომხმარებლები ან ჯგუფები ადმინისტრატორის მსგავსად);
5. აღადგინეთ Options საქალაქის თავდაპირველი კონფიგურაცია.

ამ მოქმედებათა შესრულების შედეგად ადმინისტრატორი ვეღარ შეიძლება Group Policy-ის გააქტიურებას. ამ ფუნქციის აღსადგენად კვლავ გააქტიურეთ ფანჯარა Group Policy Properties და უფლებათა ჩამონათვალიდან აირჩიეთ Full Control .

როგორ დავიცვათ თავი:

ყოველივე ზემოაღწერილის გათვალისწინებით უკვე გასაგები ხდება სისტემის უსაფრთხოების პოტენციური საფრთხეები. მეტად მნიშვნელოვანია, უსაფრთხოების ზომების დასაცავად ერთიანი გეგმის შემუშავება. გეგმაში აუცილებელია შედიოდეს შემდეგი მომენტები:

- უზრუნველყავით თქვენი კომპიუტერის ფიზიკური დაცვა;
- შეასრულეთ Windows Update დაახლოებით თვეში ერთხელ;
- გამოიყენეთ რთული პაროლები. არ გამოიყენოთ ერთი და იგივე პაროლი სხვადასხვა აღრიცხვის ჩანაწერებისათვის, შეცვალეთ პაროლები ყოველი რამოდენიმე თვის შემდეგ. არ ჩართოთ ავტომატური რეგისტრაციის რეჟიმი;
- დააყენეთ ანტივირუსული პროგრამები და რეგულარულად განაახლეთ ისინი;
- რეგულარულად შექმენით მნიშვნელოვანი მონაცემების სარეზერვო ასლები. შეინახეთ ეს ასლები უსაფრთხო ადგილას.
- მოახდინეთ მნიშვნელოვანი ინფორმაციის შიფრაცია. დეკოდირების გასაღები შეინახეთ უსაფრთხო ადგილას.
- დაიცავით უსაფრთხოების წესები ელექტრონულ ფოსტასთან მუშაობისას.

ლაბორატორიული სამუშაო №1

სამუშაოს თემა: მომხმარებელთა აღრიცხვის ჩანაწერები

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. შექმენით/წაშალეთ აღრიცხვის ჩანაწერები უტილიტით Users and Passwords;
2. შექმენით/წაშალეთ აღრიცხვის ჩანაწერები უტილიტით Local Users and Groups;
3. შექმენით/წაშალეთ აღრიცხვის ჩანაწერები Net-ბრძანებების უტილიტით;
4. შექმენით/წაშალეთ აღრიცხვის ჩანაწერები უტილიტით User Accounts;
5. გათიშეთ/ჩართეთ აღრიცხვის ჩანაწერი.

ლაბორატორიული სამუშაო №2

სამუშაოს თემა: მომხმარებელთა პაროლები.

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. ადრე შექმნილი ადრიცხვის ჩანაწერისათვის დანიშნულ პაროლი;
2. დაიცავით სისტემა Welcome ეკრანის საშუალებით;
3. გამოიტანეთ გამაფრთხილებელი შეტყობინება;
4. გამოიყენეთ თვისება Password Reset Disk;
5. გამოიყენეთ თვისება Syskey;
6. ჩართეთ პაროლების პოლიტიკა;
7. დააყენეთ მოთხოვნა რთულ პაროლზე;
8. დააყენეთ მოთხოვნა პაროლების ქრონოლოგიის ასახვის შესახებ;
9. დააყენეთ პაროლების მოქმედების მაქსიმალური ვადა ერთი კვირა.

ლაბორატორიული სამუშაო №3

სამუშაოს თემა: ღაცვის ღონისძიებები ლოკალურ ქსელში

ღავალეზა:

შეასრულეთ შემდეგი მოქმედებები:

5. ჩართეთ Simple File Sharing ინტერფეისი;
6. მიანიჭეთ თქვენს საქალაღდეს თვისება Private;
7. აღრიცხვის ჩანაწერთა ჯგუფს Users შეუზღუდეთ ინტერნეტში შესვლა;
8. აღრიცხვის ჩანაწერთა ჯგუფს Users შეუზღუდეთ Windows-ის თამაშების შესრულებაზე გაშვების უფლება;
9. აღრიცხვის ჩანაწერთა ჯგუფს Users შეუზღუდეთ პრინტერზე ბეჭდვის უფლება;
10. გათიშეთ USB-პორტის გამოყენების უფლება.

ლაბორატორიული სამუშაო №4

სამუშაოს თემა: სერთიფიკატების გამოქვნივა

ღავალაბა:

შეასრულეთ შემდეგი მოქმედებები:

1. დაათვალიერეთ სერთიფიკატები დიალოგური ფანჯრიდან Certificates და კონსოლიდან Certificates;
2. მოითხოვეთ თქვენი საკუთარი სერთიფიკატი ვებ-საიტიდან Thawte.com
3. მოახდინეთ თქვენი სერთიფიკატის ექსპორტი დისკეტზე;
4. მოახდინეთ თქვენი სერთიფიკატის იმპორტი სხვა კომპიუტერზე;
5. მოახდინეთ სერთიფიკატის კოპირება Trusted Root Certification Authorities საცავიდან Trusted People საცავში;
6. მოახდინეთ სერთიფიკატის განახლება ახალი გასაღებით;
7. გაუგზავნეთ თქვენი სერთიფიკატი რომელიმე ადრესატს Outlook Express-ის საშუალებით;
8. დაუმატეთ სხვა ადრესატის სერთიფიკატი თქვენს სერთიფიკატს;
9. წაიკითხეთ დაშიფრული შეტყობინება Outlook Express-ის საშუალებით.

ლაბორატორიული სამუშაო №5

სამუშაოს თემა: ფაილებისა და საქაღალდეების კოდირება

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. შექმენით თქვენი საქაღალდე და მასში მოათავსეთ რაიმე ფაილი;
2. დაშიფრეთ ეს საქაღალდე EPS-ის გამოყენებით;
3. მოახდინეთ ამ ფაილის დეკოდირება EPS-ის საშუალებით;
4. მოახდინეთ ფაილების კოდირება/დეკოდირება Cipher-ის საშუალებით;
5. უზრუნველყავით საერთო მიმართვა თქვენს კოდირებულ საქაღალდესთან;
6. დანიშნეთ რომელიმე აღრიცხვის ჩანაწერი მონაცემთა აღდგენის აგენტად;
7. მოახდინეთ დახურული გასაღების ექსპორტი დისკეტზე;
8. მოახდინეთ სერთიფიკატის სარეზერვო კოპირება;
9. მოახდინეთ პერსონალური სერთიფიკატის იმპორტი.

ლაბორატორიული სამუშაო №6

სამუშაოს თემა: PGP პროტოკოლის გამოყენება
დაშიფრული წერილების მიღება/გასაბზავნად.

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. მოახდინეთ PGP-ის ინსტალაცია;
2. მოახდინეთ გასაღების გენერაცია;
3. გაგზავნეთ ღია გასაღები სერვერზე Global Directory;
4. დაშიფრეთ ინფორმაციის PGP-ის საშუალებით;
5. გაუგზავნეთ ეს ინფორმაცია ადრესატს;
6. მოახდინეთ დაშიფრული ინფორმაციის დეშიფრაცია;
7. მოახდინეთ CertifiedMail.com პროგრამის ინსტალაცია
საიტიდან <http://www.certifiedmail.com>;
8. გამოიყენეთ ეს სამსახური ინფორმაციის კოდირება/
დეკოდირებისათვის.

ლაბორატორიული სამუშაო №7

სამუშაოს თემა: მონაცემთა დაცვა

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. შექმენით მონაცემთა სრული (Normal) სარეზერვო ასლი Windows Backup-ის საშუალებით;
2. შექმენით მონაცემთა დამატებითი (Incremental) სარეზერვო ასლი Windows Backup-ის საშუალებით;
3. შექმენით მონაცემთა დიფერენცირებული (Differential) სარეზერვო ასლი Windows Backup-ის საშუალებით;
4. აღადგინეთ მონაცემები Windows Backup-ის სარეზერვო ასლიდან;
5. გამოიყენეთ უტილიტა Chkdsk;
6. გააქტიურეთ უტილიტა System Restore;
7. მოახდინეთ Windows-ის განახლება უტილიტით Windows Update;
8. შეამოწმეთ თქვენი კომპიუტერის მდგომარეობა MBSA უტილიტის საშუალებით;
9. შეამოწმეთ ქსელის ყველა კომპიუტერი MBSA უტილიტის საშუალებით;
10. აამუშავეთ MBSA უტილიტა ბრძანებათა სტრიქონიდან, გამოიყენეთ მისი სხვადასხვა პარამეტრები.

ლაბორატორიული სამუშაო №8

სამუშაოს თემა: მოვლენათა აუდიტი

ღავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. ჩართეთ აღრიცხვის ჩანაწერების რეგისტრაციის მოვლენათა აუდიტი. დააფიქსირეთ User-ი, რომელიც ცდილობდა ადმინისტრატორის აღრიცხვის ჩანაწერით დარეგისტრირებას;
2. ჩართეთ აღრიცხვის ჩანაწერების მართვის აუდიტი. დააფიქსირეთ User-ი, რომელიც ცდილობდა ახალი აღრიცხვის ჩანაწერის შექმნას;
3. ჩართეთ პოლიტიკის შეცვლის აუდიტი; დააფიქსირეთ User-ი, რომელიც ცდილობდა აუდიტის და პაროლების პოლიტიკის შეცვლას;
4. ჩართეთ ობიექტებთან მიმართვის აუდიტი. დააფიქსირეთ User-ი, რომელიც ცდილობდა აკრძალული ფაილის და საქაღალის დათვალიერებას;
5. დაათვალიერეთ აუდიტის ჟურნალი, გაფილტრეთ მოვლენების მიხედვით;
6. უსაფრთხოების ჟურნალში შეცვალეთ პარამეტრები, ისე რომ მოვლენები ინახებოდეს 10 დღე.

ლაბორატორიული სამუშაო №9

სამუშაოს თემა: უსაფრთხოების პოლიტიკები

დავალება:

შეასრულეთ შემდეგი მოქმედებები:

1. დაბლოკეთ Gest აღრიცხვის ჩანაწერი;
2. საშუალებას იძლევა ადმინისტრატორის აღრიცხვის ჩანაწერს შეეცვალოს სახელი;
3. გააქტიურეთ პოლიტიკა, რომელიც გათიშავს სისტემას იმ შემთხვევაში თუ არ მოხდება უსაფრთხოების ჟურნალში ჩანაწერების ჩაწერა;
4. გააქტიურეთ პოლიტიკა, რომელიც Windows-ში ყოველი რეგისტრაციისას გამოიტანს გამაფრთხილებელ შეტყობინებას.
5. გათიშეთ ღილაკი Shut Down დიალოგურ ფანჯარაში Log On To Windows;
6. გააქტიურეთ პოლიტიკა, რომელიც კოდირების ფაილური სისტემის (EPS) ნაცვლად გამოიყენებს 3DES სტანდარტს ფაილების კოდირება/დეკოდირებისათვის.

ლაბორატორიული სამუშაო №10

ჯგუფური კოლიტიკების გამოქმენებით შეასრულეთ შემდეგი მოქმედებები:

1. აკრძალეთ Control Panel-თან მიმართვა;
2. დამალეთ My Computer საქაღალდეში D: დისკი ;
3. გათიშეთ Certificates დილაკი, რომელიც გამოსახულია დიალოგური ფანჯრის Content ჩანართში;
4. გააქტიურეთ პოლიტიკა, რომელიც კრძალავს თქვენს მიერ ვებ-გვერდებზე აკრებილი პაროლების დამახსოვრებას;
5. აუკრძალეთ მომხმარებელს Internet Explorer-ის უსაფრთხოების ზონების დათვალიერება და შეცვლა;
6. დაბლოკეთ ბრძანებათა სტრიქონიდან პროგრამების გაშვების უფლება;
7. დაბლოკეთ რეესტრის რედაქტორის გამოყენების უფლება;
8. გააქტიურეთ პოლიტიკა, რომელიც დამალავს Security ჩანართს ობიექტების თვისებების დიალოგური ფანჯრიდან;
9. გააქტიურეთ პოლიტიკა, რომელიც პაროლით დაიცავს ყველა Screen Saver-ს.
10. Windows-ის Start დილაკში გამოაჩინეთ მხოლოდ ის პროგრამები, რომელთა გაშვების უფლებასაც აძლევთ მომხმარებელს.

ლიტერატურა

1. გ. ჩოგვაძე, გ. გოგიჩაიშვილი, გ.სურგულაძე, თ. შეროზია, ო.შონია. მართვის ავტომატიზებული სისტემების დაპროექტება და აგება, თბილისი, 2001წ.
2. კობტჰე, გ.სურგულაძე, თ.დოლიძე, ო.შონია თანამედროვე პროგრამული პროლატორები და ენები, თბილისი, „ტექნიკური უნივერსიტეტი“ 2003წ.
3. გ.გოგიჩაიშვილი, კ.ოდიშარია, ო.შონია. ინფორმაციის დაცვა ავტომატიზებულ სისტემებში, თბილისი, საქართველოს ტექნიკური უნივერსიტეტი, 2008წ.
4. ო.შონია, თ.შეროზია. ინფორმაციული ტექნოლოგიები და უსაფრთხოება. თბილისი, საქართველოს ტექნიკური უნივერსიტეტი, 2008წ.
5. გ.სურგულაძე, ო.შონია, ლ. ყვავაძე, მონაცემთა განაწილებული ბაზების მართვის სისტემები, თბილისი 2004წ.
6. ო.შონია, გ.ნარეშელაშვილი, ი.ქართველიშვილი, უმავრთული ქსელების უსაფრთხოება, თბილისი, ტექნიკური უნივერსიტეტი, 2009.
7. Э.Ботт, К.Зихерт, Безопасность Windows, 2003.
8. Использование PGP
http://old.pgpru.com/pgp_for_beginners/pgp_for_beg_04.htm.