**ლექცია №5 აუდიტის პოლიტიკა**

სხვადასხვა აღრიცხვის ჩანაწერების გამოყენება იძლევა საშუალებას გაკონტროლდეს მათი მფლობელების ქმედებები კომპიუტერთან მუშაობისას, ინფორმაციული უსაფ­რთხოების თვალსაზრისით..

ის მოქმედებები (მოვლენები) რომლებიც მიმდინარეობა კომპიუტერში, მონიტორინ­გის დაექვემდებარება ორი საშუალებით:

* **აუდიტის მითითება** - ამ პროცესით ხდება კომპიუტერში მიმდინარე მოვლენების, ქმედებების დაფიქსირება - ჩაწერა რაიმე ჟურნალში;
* **მოვლენათა დათვალიერება (Event Viewer) -** ამ უტილიტას გამოყენებით ხდებააუდიტის ფაილებში არსებული ჩანაწერების დათვალიერება.

**I.** აუდიტის მითითება ხდება შემდეგი სქემის (ალგორითმის გამოყენებით) :

**Start »Control Panel » Administrative Tools » Local Security Setting » Local Policies » Audit Policy**

ან ბრძანები სტრიქონში ბრძანების- **secpol.msc** აკრეფით



ნახატი 5.1 აუდიტის პოლიტიკის არჩევა

ლოკალური უსაფრთხოების პარამეტრებში (Local Security Setting) მარცხენა მხარეს არჩეულია აუდიტის პოლიტიკა, ხოლო მარჯვენა სვეტში იმ მოვლენათა ჩამონათვალია, რომელთა აუდიტის მითითებაა შესაძლებელი. მაგალითად, მოვლენის - სისტემაში შესვლის აუდიტის მითითებისთვის საჭიროა შევიდეთ *სისტემაში შესვლის აუდიტში (Audit account logon events)* – დავაწკაპუნოთ შესაბამის აპლეტზე, გაიხსნება ფანჯარა - *Audit account logon events Properties - სისტემაში შესვლის აუდიტის თვისებები .*



ნახატი 5.2. სისტემაში შესვლის აუდიტის თვისებები

დიალოგის რეჟიმში შეგვიძლია ავირჩიოთ აუდიტი აღსრულებული თუ არ აღსრულებუ­ლი მოვლენების, ან ორივეს ერთდროულად. პირველ შემთხვევაში ვაყენებთ აღნიშვნას ***წარმატების*** (Success) კვადრატში, მეორე შემთხვევაში ვაყენებთ აღნიშვნას ***წარუმატების*** (Failure) კვადრატში, მესამე შემთხვევისთვის ორივე კვადრატში ვსვამთ აღნიშნას.

ჩამოვთვალოთ ის მოვლენები, რომლებიც შეიძლება ჩაწერილ იქნენ უსაფრთხოების ჟურნალში:

* ***სისტემაში შესვლის აუდიტი*** *(Audit account logon events)* - აფიქსირებს ლოკალური კომპიუტერის სისტემაში აღრიცხვის ჩანაწერებით შესვლას.
* ***აღრიცხვის ჩანაწერების მართვის აუდიტი*** *(Audit account management)* - აფიქსირებს აღრიცხვის ჩანაწერში შეტანილ ცვლიცებებს.
* ***კატალოგთა სამსახურის წვდომის აუდიტი*** *(Audit directory service access) –* თუ კი კომპიუტერი *Active directory* დომენის ნაწილია, ეს პუნქტი საშუ­ალებას იძლევა აუდიტის ფაილში დაფიქსირდეს წვდომა დირექტორიის ნებისმიერი ობიექტისადმი, რომელთაც აქვთ წვდომის მართვის სისტემური ცხრილი *(SA*CL).
* ***სისტემაში შესვლის მოვლენათა აუდიტი*** *(Audit logon events) -* აფიქსირებს სისტემაში ლოკალურ და ქსელურ შესვლებს.
* ***ობიექტებისადმი წვდომის აუდიტი*** *(Audit object access) -* აფიქსირებს ნებისმიერი ობიექტისადმი წვდომას, რომელთაც აქვთ ცხრილი *(SA*CL).
* ***პოლიტიკის შეცვლის აუდიტი*** *(Audit policy change) –* აფიქსირებს პოლიტიკის ნებისმიერ ცვლილებას, მათ შორის აუდიტის პოლიტიკის ცვლილებას, მომხმარებლისათვის უფლებების მინიჭებისა და სხვა ცვლილებებს.
* ***პრივილეგიების გამოყენების აუდიტი*** *(Audit privilege use) -* აფიქსირებს უფლებების ყოველ გამოყენებას. მისი სრული ჩართვა მალე გაავსებს ჩანაწერებით ჟურნალს. ამიტომაც უმჯობესია მხოლოდ წარუმატებწლი მცდელობების ფიქსაციის რეჟიმის ჩართვა.
* ***პროცესების მეთვალყურეობის აუდიტი*** *(Audit process tracking) -* აფიქსირებს ყოველ გაშვებულ პროცესს.
* ***სისტემური მოვლენების აუდიტი*** *(Audit system events) –აფიქსირებს იმ მოვლენებს, რომლებმაც იქონიეს ზემოქმედება სისტემის უსაფრთხოებაზე* *ან უსაფრთხოების რეგისტრაციის ფაილზე.*

**II. მოვლენათა დათვალიერების პროგრამა (Event Viewer)** იძლევა საშუალებას აუდი­ტის მითითების პოლიტიკის ჩართვის შედეგად დაფიქსირებული მოვლენების აღ­მწერი ჩანაწერების დათვალიერებისა. და არა მარტო მათი. მოვლენათა დათვალი­ერების პროგრამით შესაძლებელია სამი ტიპის მოვლენების ჩანაწერების ჟურნალის ფაილების დათვალიერება:

* მოვლენები, რომლებიც უსაფრთხოებასთანაა დაკავშირებული;
* სისტემური მოვლენები;
* მოვლენები, დაკავშირებულნი გამოყენებითი პროგრამების გაშვებით.

აღსანიშნავია, რომ ჩუმათობის პრინციპით სისტემა არა ყველა მოვლენას აფიქსირებს. ასე მაგალითად აუცილებელია ჯგუფების პოლიტიკის მეშვეობით გახდეს შესაძლე­ბელი უსფრთხოების მოვლენების პროტოკოლირება, რაზეც საუბარი იყო წინა ორ ლექციებში.

მოვლენათა დათვალიერების პროგრამის გასაშვებლად საჭიროა შემდეგი სქემის შესრულება **Start »Control Panel » Administrative Tools » Event Viewer** ნახატი 5.3. ან ბრძანების სრტიქონში ავკრიფოთ - **eventvwr.exe,** მოვლე­ნების დათვალიერების მარცხენა სვეტში მოცემულია მოვლენათა ჩაწერის ჟურნალთა ჩამო­ნათვალი, როგორც წესი სამი აუცილებელი - გამოყენებითი პროგრამების გაშვების ( application log file), სისტე­მური (system log file), უსაფრთხოების (security log file) და ამ შემთხვევაში კიდევ სამი ჟურ­ნალი - Doctor Web, Microsoft Office Diagnostics, Microsoft Office Sessions. მარჯვენა მხარეს კი როცა დავაწკაპუნებთ რომელიღაც ჟურნალზე, გაიხსნება მასში ჩანაწერების უფრო მეტი დეტალები, ნახატი 5.4.

თუ კი ამ დეტალურ ჩანაწერზე ორჯერ დავაწკაპუნებთ, მაშინ გაიხსნება სრული ჩანაწერი ამ მოვლენისა. ნახატი 5.5, 5.6 - რომლებშივ შესაბამისად მოცემულია წარუმატებელი და წარმატებული მოვლენები.



ნახატი 5.3. მოვლენათა დათვალიერება



ნახატი 5.4



ნახატი 5.5



ნახატი 5.6

იმის მისათითებლად თუ რა ტიპის მოვლენასთა გვაქვს საქმე, შემოტანილია ტიპების ცნება, რომელიც მარჯვენა სვეტში იწერება. განვიხილოთ ისინი

* შეცდომა (Error) -მისი სიმბოლოა  და რაღაც მნიშვნელოვან მოვლენაზეა საუბარი.
* გაფრთხილება (Warning)- მისი სიმბოლოა  , მიუთითებს პრობლემებზე, მაგრამ არა იმდენად სერიოზულზე, რომ ჩათვალო როგორც შეცდომა. მაგალითად ის შეიძლება დაფიქსირდეს, როცა სისტემა აღმოაჩენს, რომ მყარ დისკზე დარჩა მცირე ზომის თავისუფალი მეხსიერება.
* შეტყობინება (Information) მისი სიმბოლოა - 
* შესვლის წარმატებული მცდელობა ( Success audit) - მისი სიმბოლოა 
* შესვლის წარუმატებული მცდელობა (Failure audit) - მისი სიმბოლოა 

Windows-ის ჩატვირთვისთანავე სტარტს იღებს ***მოვლენათა პროტოკოლირების სამსახური*** , რომელიც კომპიუტერის მუშაობის პირველივე წამებიდან აფიქსირებს იმ მოვლენებს, რომელსაც ადგილი ჰქონდა მუშაობის პროცესში. ამასთან ის მოვ­ლენები, რომლებიც ჩუმათობის პრინციპით ფიქსირდება, მაგალითად სისტემური და გამოყენებითი, მოვლენათა დათვალიერების პროგრამით შეძლება ნახოს ნე­ბისმიერმა მომხმარებელმა, ხოლო ის მოვლენები, რომლებიც ინიცირდება, მაგა­ლითად უსაფრთხოების შეუძლია ნახოს მხოლოდ ადმინისტრატორმა.

**III. ფაილებსა და საქაღალდეებზე წვდომის აუდიტი.**

კონტროლის დასამყარებლად იმაზე. თუ ვინ, და როგორ სარგებლობს, ამა თუ, იმ საქაღალდეთი ან ფაილით, თავდაპირველად აუცილებელია ფაილებზე მარტივი ზო­გადი წვდომის (Simple File Sharing) გამორთვა, რადგანაც ის არ აჩენს უსაფრთხო­ების (Security) ჩანართს ფაილებისა და საქაღალდეების თვისებების (Properties) დიალო­გურ ჩანართში.

Simple File Sharing –ის გამოსართავად, მოვიქცეთ შემდეგნაირად:

1. გავხსნათ Windows Explorer (ვინდოუსში გამცილებელი) : start » accessories » Windows Explorer

2. ავირჩიოთ Tools/Folder Options (სერვისი/საქაღალდეთა თვისებები)

3. ავირჩიოთ Folder Options -ში view და იქ გამოვრთოთ ოპცია User simple file sharing (Recommended)