Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 2

*Metode și mijloace tehnice de protecție a informației.*

A efectuat: st. gr. SI-211 Chirița Stanislav

A verificat: dr. conf.univ. Colesnic Victor

Chișinău – 2024

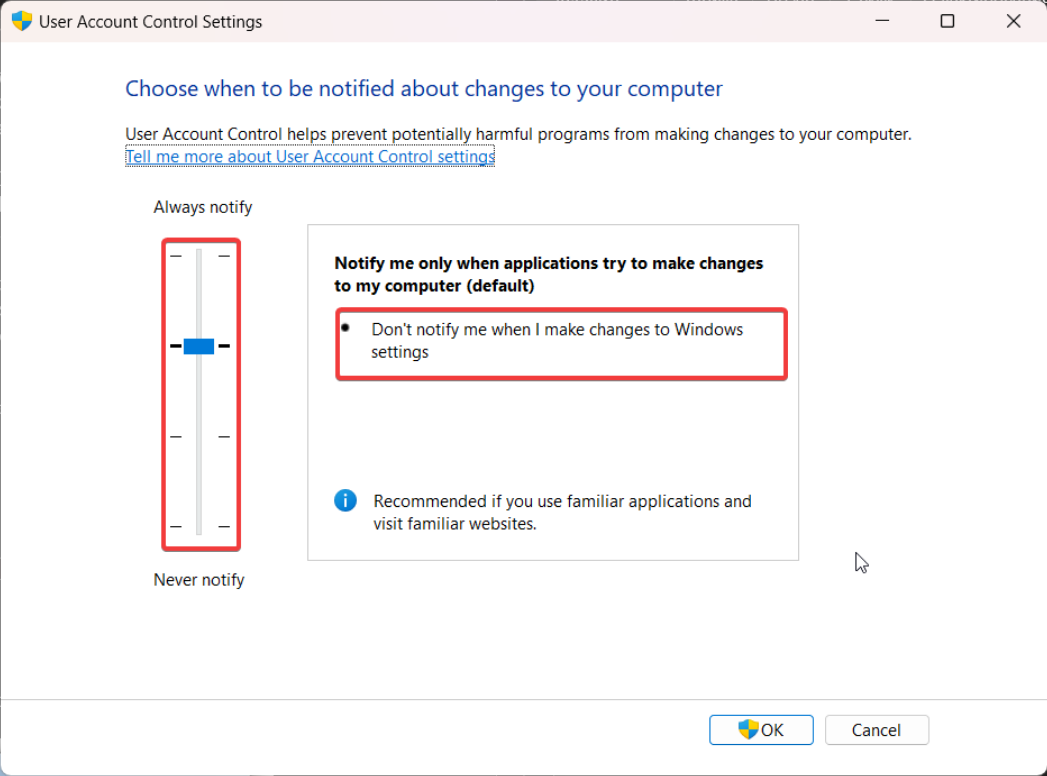
**Lucrare de laborator 2**

**Tema:** **Gestionarea conturilor utilizatorilor în Windows,**

**studierea** Windows Registry

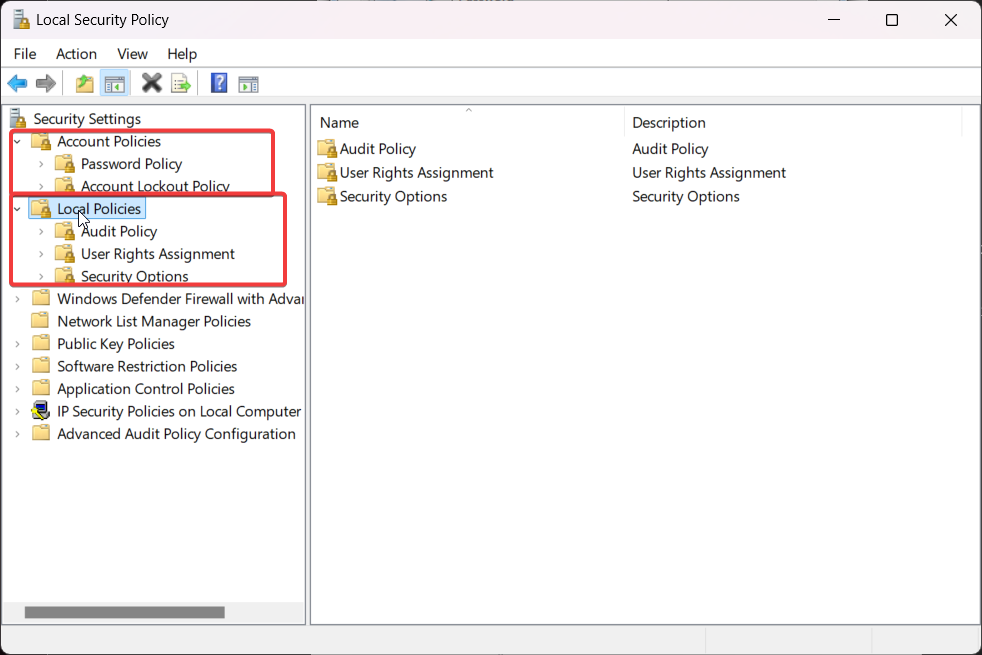
**Scopul lucrării**: Cunoașterea procedurii de gestionare a conturilor utilizatorilor și a permisiunilor acestor conturi, abilități de detectare a programelor malware utilizând Windows Registry.

Figura 1.1 arată fereastra de setări "User Account Control Settings" din Windows, unde utilizatorul poate alege când să fie notificat despre modificările făcute pe computer. În partea stângă, există un glisor care reglează nivelul de notificare. Glisorul este setat pe opțiunea implicită, care notifică utilizatorul doar când aplicațiile încearcă să facă modificări în sistem, dar nu și atunci când utilizatorul modifică setările Windows.



*Figura 1.1 UAC*

Imaginea din Figura 1.2 afișează consola „Local Security Policy” deschisă folosind comanda secpol.msc în Windows. În partea stângă, este selectată secțiunea „Local Policies”, care include „Audit Policy”, „User Rights Assignment” și „Security Options”. Aceste setări permit configurarea politicilor locale de securitate pe sistem, inclusiv drepturile utilizatorilor și opțiunile de securitate avansate.



*Figura 1.2 -* Local Security Policy (secpol.msc)

2. **Operarea cu Windows Registry**

Imaginile anexate ilustrează diferite panouri și console utilizate pentru gestionarea politicilor de securitate și configurarea sistemului.

**User Account Control Settings**  
Această imagine prezintă fereastra „User Account Control” (UAC), care permite utilizatorului să seteze nivelul de notificare atunci când se efectuează modificări la nivel de sistem. UAC este un mecanism important pentru prevenirea schimbărilor neautorizate, protejând astfel integritatea sistemului.

**Local Security Policy**  
Această captură de ecran arată consola secpol.msc, utilizată pentru gestionarea politicilor de securitate locale. Setările vizibile includ „Audit Policy”, „User Rights Assignment” și „Security Options”, care sunt esențiale pentru controlul drepturilor utilizatorilor și auditarea activităților în sistem.

**Registry Editor**  
Editorul de Registru din imagine este un instrument esențial pentru administrarea configurărilor avansate din Windows. Aici se pot face modificări directe asupra cheilor de registru, cum ar fi cele din HKEY\_LOCAL\_MACHINE și HKEY\_CURRENT\_USER, care influențează comportamentul aplicațiilor și al sistemului de operare.

Изображение выглядит как текст, программное обеспечение, компьютер, Значок на компьютере

Автоматически созданное описание

Figura 2.1 – Registry Editor (regedit)

**Elemente cheie:**

* **Fereastră principală:** Titlul ferestrei indică faptul că este o secțiune din Editorul de Registru Windows. Editorul de Registru este o bază de date care stochează setările de configurare pentru hardware, software și utilizatori pentru sistemul de operare Windows.
* **Arborele de directoare:** În partea stângă, este prezentat un arbore de directoare care afișează structura organizată a cheilor și subcheilor din registru. Calea completă afișată este: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Aceasta indică faptul că imaginea prezintă setările specifice pentru procesul Winlogon, care este responsabil pentru gestionarea sesiunilor de conectare ale utilizatorilor.
* **Panoul de detalii:** În partea dreaptă, este afișat panoul de detalii care prezintă valorile asociate cu cheile selectate din arborele de directoare. Fiecare rând reprezintă o intrare în registru, iar coloanele indică numele valorii, tipul de dată, și valoarea în sine.
* **Valorile de registru:** Valorile afișate în panoul de detalii pot include informații despre setările automate de conectare, opțiuni de pornire, configurații de securitate și alte aspecte legate de procesul Winlogon.

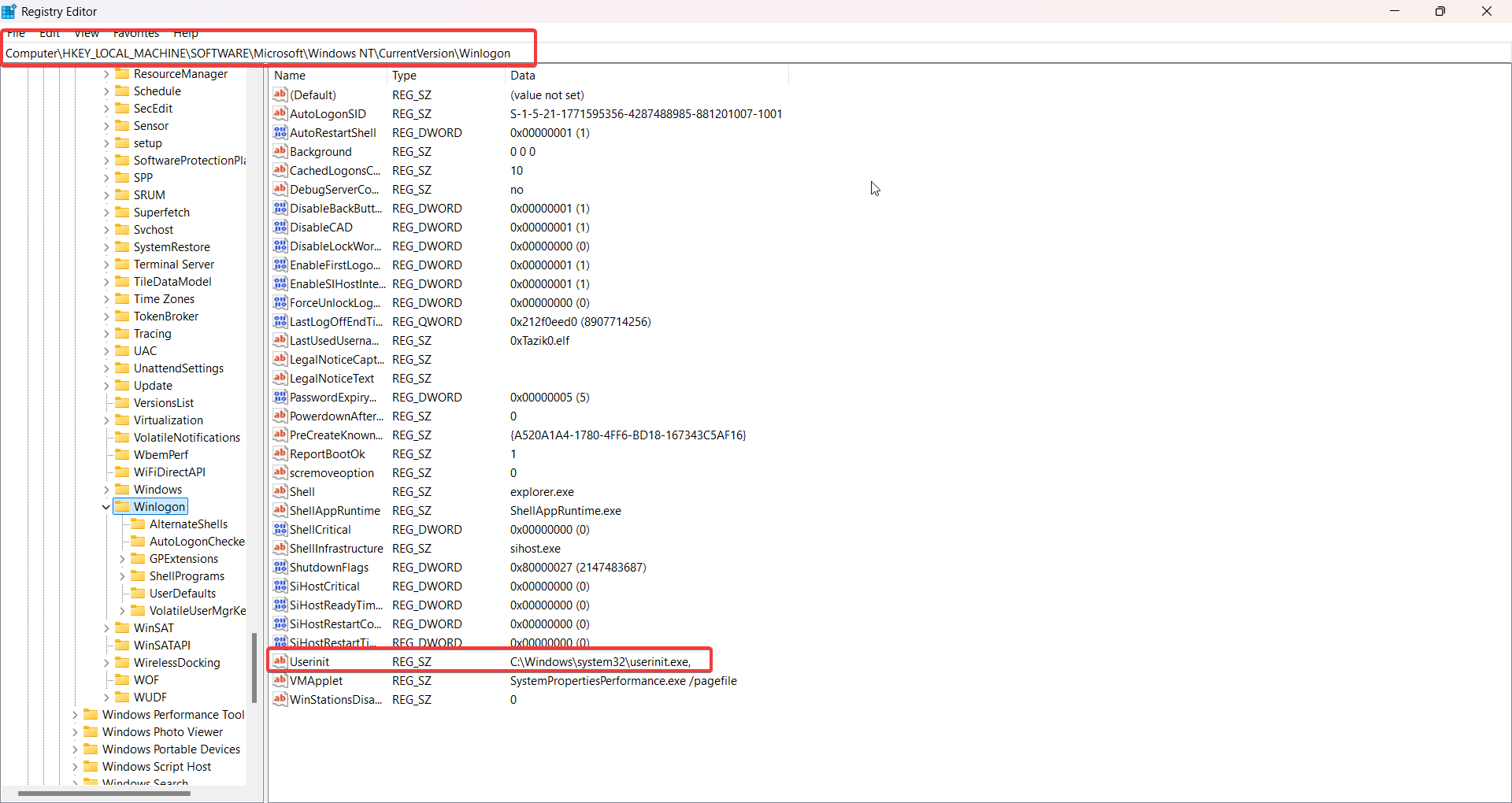


Figura 2.2 – **Userinit**

Impactul modificării valorii "Userinit"

Modificarea valorii "Userinit" poate avea o gamă largă de efecte, în funcție de conținutul exact al fișierului specificat. Iată câteva scenarii posibile:

Executarea automată de programe:

* + Exemple: Antiviruși, utilitare de backup, aplicații de comunicare.
  + Beneficii: Automatizarea sarcinilor, asigurarea securității.
  + Riscuri: Poate încetini procesul de logare, poate cauza conflicte între aplicații.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Figura 2.3 – Userinit(Edit)

**Ce înseamnă aceste erori?**

* **Erori de registru:** Acestea indică probleme în baza de date a sistemului de operare, unde sunt stocate setările pentru programe și hardware. De obicei, aceste erori apar după dezinstalarea incompletă a programelor sau după modificări neautorizate în registru.
* **Fișiere invalide:** Acestea sunt fișiere care nu mai sunt necesare sau care sunt corupte și pot afecta stabilitatea sistemului.
* **Date lipsă:** Acestea se referă la informații care ar trebui să fie prezente în registru, dar lipsesc, ceea ce poate duce la funcționarea incorectă a anumitor programe.

**Ce recomandă programul?**

Programul sugerează diverse acțiuni pentru a remedia aceste probleme, în principal ștergerea cheilor de registru invalide și a fișierelor inutile.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Figura 2.4 -jv16 Scan

Concluzie: În concluzie, controlul contului în Windows și Local Security Policy joacă un rol esențial în securizarea accesului și gestionarea politicilor de securitate la nivel local, permițând utilizatorilor să stabilească permisiuni și restricții pentru protejarea sistemului împotriva activităților neautorizate. Windows Registry, cu structura sa pe secțiuni, reprezintă un element central al configurației sistemului de operare, unde modificările pot afecta în mod semnificativ funcționarea acestuia. Intervențiile asupra cheilor Registry, fie pentru optimizarea performanței, fie pentru depistarea malware-ului, trebuie realizate cu prudență, deoarece o modificare greșită poate destabiliza sistemul.

Utilizarea unor instrumente de optimizare, cum ar fi jvl6 Power Tools, demonstrează cum uneltele software moderne pot contribui la întreținerea și îmbunătățirea performanței sistemului, prin curățarea registrului, eliminarea fișierelor inutile și ajustarea setărilor avansate. Aceste acțiuni nu doar că îmbunătățesc viteza și stabilitatea, ci și protejează împotriva vulnerabilităților pe termen lung.

În ansamblu, gestionarea corespunzătoare a setărilor de securitate, a registrului Windows și folosirea unor unelte adecvate pentru optimizare reprezintă factori critici în menținerea securității și performanței optime a unui sistem de operare Windows.