

Лабораторна робота №4

Тема: Системний реєстр.

Мета: Вивчити призначення та методи роботи з системним реєстром Windows.

Завдання.

1. Вивчити призначення та структуру системного реєстру.

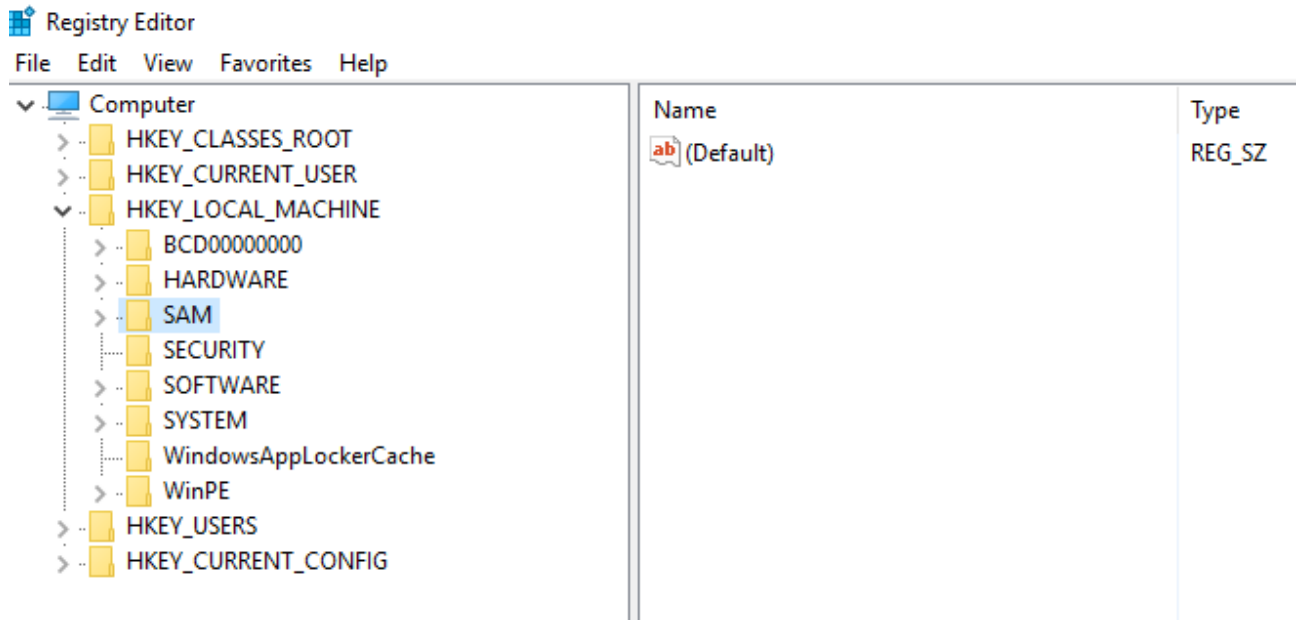
Реєстр Windows — це централізована база даних, яка зберігає конфігураційні параметри та налаштування операційних систем Microsoft Windows. У ньому міститься інформація про апаратне забезпечення, програмне забезпечення, облікові записи користувачів і системні параметри. Зміни, які користувач вносить через «Панель керування» або інші засоби конфігурації, автоматично фіксуються в реєстрі.

Реєстр структурований у вигляді декількох основних розділів:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

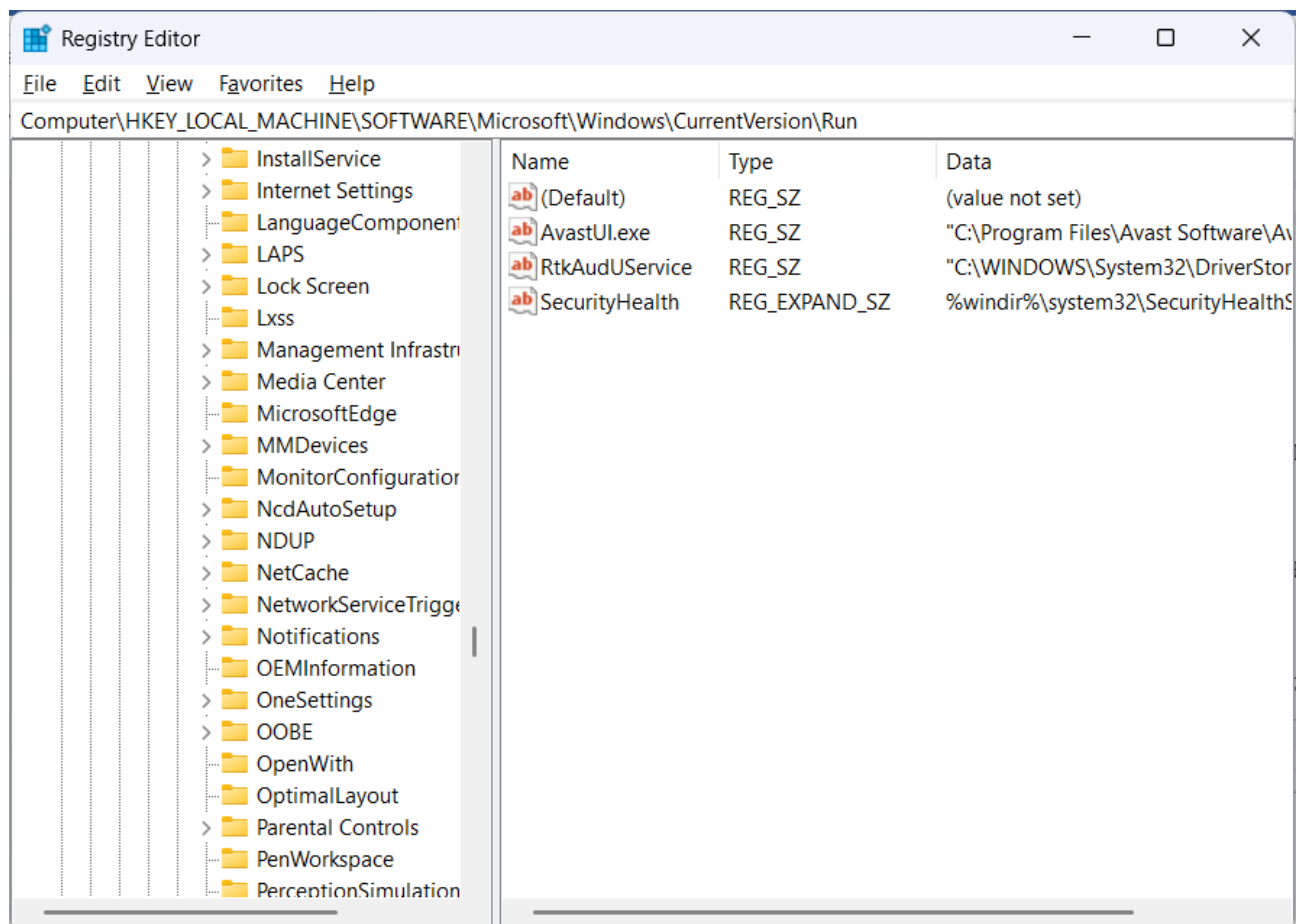
2. Вивчити призначення та методи роботи з утилітою RegEdit.

RegEdit — це утиліта операційної системи Windows, яка забезпечує доступ до системного реєстру для його перегляду та редагування. За допомогою цього інструменту можна створювати, змінювати, імпортувати та експортувати ключі й значення реєстру. Використовувати утиліту слід обережно, оскільки неправильні зміни можуть призвести до збоїв у роботі системи.

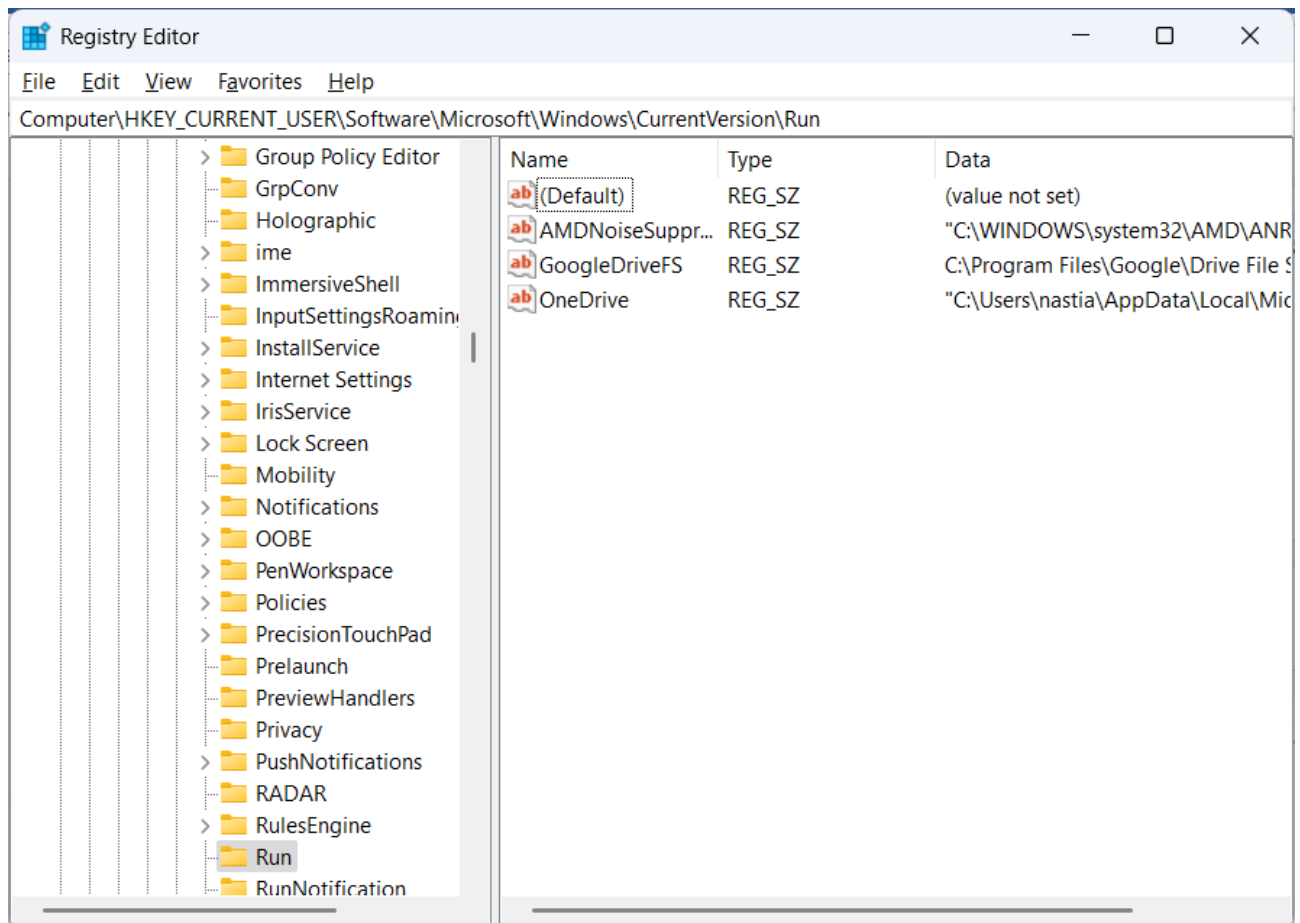


3. Знайти відповідні розділи реєстру в яких є інформація про програми та служби які завантажуються автоматично.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



4. Програмно, вивести список усіх програм та служб які завантажуються автоматично для усіх користувачів та поточного користувача.

```
C:\lab4>4.cmd
Автозавантаження: поточний

OneDrive       : "C:\Users\nastia\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
GoogleDriveFS  : C:\Program Files\Google\Drive File Stream\107.0.3.0\GoogleDriveFS.exe --startup_mode
AMDNoiseSuppression : "C:\WINDOWS\system32\AMD\ANR\AMDNoiseSuppression.exe"
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
PSCildName     : Run
PSDrive       : HKCU
PSProvider    : Microsoft.PowerShell.Core\Registry

Автозавантаження: усі

SecurityHealth : C:\WINDOWS\system32\SecurityHealthSystray.exe
RtkAudUService : "C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_c607c18cb15933d8\RtkAudUService64.exe" -background
AvastUI.exe    : "C:\Program Files\Avast Software\Avast\AVLaunch.exe" /gui
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
PSCildName     : Run
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

Лістинг коду:

```
@echo off
chcp 65001 >nul
powershell -Command "Write-Output 'Автозавантаження: поточний'; Get-ItemProperty HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
powershell -Command "Write-Output 'Автозавантаження: усі'; Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Run"
```

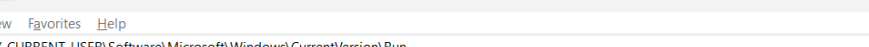
5. Додати програмно до автозавантаження програм для поточного користувача завантаження програми WinWord або іншої.

```
C:\lab4>5.cmd
The operation completed successfully.
Програма SuperWord додана.
```

Лістинг коду:

```
@echo off
chcp 65001 >nul
REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /V "SuperWord" /t
REG_SZ /d "\"C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE\""" /f
echo Програма SuperWord додана.
```

6. Вивести список повторно, та показали що зареєстрована програма є у списку.



The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure, with the path `Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` selected. The right pane shows a list of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
AMDNoiseSuppr...	REG_SZ	"C:\WINDOWS\system32\AMD\ANR\AMDNoiseSu...
GoogleDriveFS	REG_SZ	C:\Program Files\Google\Drive File Stream\107.0.3...
OneDrive	REG_SZ	"C:\Users\nastia\AppData\Local\Microsoft\OneDri...
SuperWord	REG_SZ	"C:\Program Files\Microsoft Office\root\Office16\...

Реєстрація успішно.

7. Вивести список усіх завдань, які зареєстровані у планувальнику задач системи. Інформації отримати з відповідного розділу реєстру, як для усіх користувачів так і для поточного користувача.

[illegible]

Лістинг коду:

```
@echo off
chcp 65001 >nul
echo Усі:
reg query "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree"
echo Поточний:
reg query "HKCU\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree"
pause
```

8. Зробити програмно копію будь якого розділу реєстру у файл відповідного формату .reg

```
C:\lab4>8.cmd

C:\lab4>reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" backup.reg
The operation completed successfully.
```

Лістинг коду:

```
reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" run_backup.reg
```

9. За допомогою текстового редактора створити REG файл, за допомогою якого в реєстр у відповідний розділ буде внесено інформацію про асоціацію відкриття файлів .ttt програмою notepad.

Лістинг коду:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\.ttt]

@="tttfile"

[HKEY_CLASSES_ROOT\tttfile\shell\open\command]

@="notepad.exe \"%1\""

10. Описати усі виконані дії у звіті.

Висновок: Під час виконання лабораторної роботи було створено багаторівневий скрипт обслуговування системи.