Міністерство освіти і науки України
Національний авіаційний університет
Навчально-науковий інститут комп'ютерних інформаційних технологій
Кафедра комп'ютеризованих систем управління

# Лабораторна робота №7
з дисципліни «Діагностика та експлуатація комп'ютера»
на тему «Дослідження реєстру операційної системи Windows»

Виконав:
студент ННІКІТ
групи СП-325
Клокун В. Д.
Перевірив:
Масловський Б. Г.

Київ 2018

## 1 Ціль роботи

Ознайомлення з реєстром операційної системи Windows. Вивчення структури, параметрів та методів редагування.

## 2 Короткі теоретичні відомості

Реєстр Windows являє собою базу даних, що зберігає параметри і налаштування для операційних систем Microsoft Windows 32-бітних версій, 64-бітних версій та Windows Mobile/Windows Phone. Він містить інформацію і параметри налаштування для всіх апаратних засобів, програмного забезпечення, користувачів тощо. Кожен раз, коли користувач змінює будь-які параметри в "Панелі керування", зміни відбуваються у реєстрі. Реєстр Windows було введено, щоб відмовитись від використання файлів INI, що використовувалися для збереження параметрів конфігурації програм Windows раніше (тобто кожна програма зберігала свої настроювання в окремому файлі). Тому ці файли мали тенденцію бути розкиданими по всій системі, що робило важким спостереження і контроль за ними.

Реєстр можна розглядати як записну книжку Windows — як тільки системі потрібна якась інформація, вона шукає її в реєстрі. Реєстр дуже великий, і дати однозначне його визначення неможливо. Стисло й досить точно можна сказати, що реєстр — компонент операційної системи комп'ютера, який в ієрархічній базі даних зберігає найважливіші установки та інформацію про додатки, системних операціях, користувальницької і апаратної конфігураціях.

В ОС Windows NT (2000 / XP) і Vista (Vista / 7) реєстр зберігається в спеціальному каталозі `System32\Config`, який зберігає у вигляді захищених файлів розділи реєстру.

В цілому реєстр дуже нагадує файлову систему з тією різницею, що замість файлів на нижньому рівні містяться параметри.

Інформація, що зберігається в ієрархічній базі даних реєстру, зібрана в розділи (key), які містять один або більше підрозділів (subkey). Кожен підрозділ містить параметри (value).

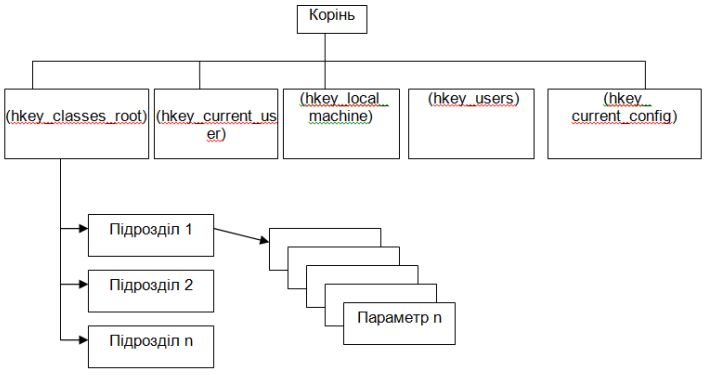


Рис. 1: Оглядовий приклад структури реєстру

Весь реєстр Windows Vista ділиться на п'ять основних. Базову структуру реєстру формують саме ці розділи:

— KEY_CLASSES_ROOT (HKCR);
— KEY_CURRENT_USER (HKCU);
— KEY_LOCAL_MACHINE (HKLM);
— KEY_USERS (HKU);
— KEY_CURRENT_CONFIG (HKCC).

HKEY_CLASSES_ROOT — це розділ реєстру, в якому містяться відповідності між різними розширеннями файлів і стосуються цих розширень додатками. Дані взаємозв'язку між розширеннями файлів і додатками дозволяють коректно відкривати файли. Приміром, в даному розділі реєстру встановлюється відповідність між розширенням * .doc і додатком Word.Document.8. В результаті всі файли з розширенням * .doc відкриватимуться за допомогою додатка Word.

Дані відповідності між розширеннями файлів і додатками зберігаються також в двох інших розділах реєстру:

1. HKLM\Software\Classes;
2. HKCU\Software\Classes.

Розділ HKLM\Software\Classes містить параметри за замовчуванням, які стосуються усіх користувачів локального комп'ютера.

В розділ HKCU\Software\Classes включені параметри, які відрізняються від стандартних параметрів і відносяться тільки до активного користувача.

В розділі HKCR зберігаються дані як з розділу HKLM\Software\Classes, так і з розділу HKCU\Software\Classes.

HKEY_CURRENT_USER - це розділ реєстру, в якому містяться дані про поточного користувача комп'ютера. Тут зберігаються папки користувача, налаштування екрану, робочий стіл і т.д., а крім того - параметри, які використовуються різними додатками.

Найбільш корисним в даному розділі є підрозділ Software, що включає параметри, що відносяться до кожного з встановлених в системі додатків.

HKEY_LOCAL_MACHINE - це розділ реєстру, в якому зберігається інформація про апаратну конфігурації ПК, яка є абсолютно однаковою для всіх користувачів ПК.

HKEY_USERS - це розділ реєстру, в якому містяться всі профілі користувачів комп'ютера, підрозділом якого є по суті розділ HKEY_CURRENT_USER.

HKEY_CURRENT_CONFIG - це розділ реєстру, в якому містяться відомості про профіль обладнання, який використовується локальним комп'ютером при запуску системи.

Можливість створювати вкладені підрозділи дозволяє групувати параметри і у результаті виходить деревоподібна структура, яку можна переглянути в «Редакторі реєстру» (Registry editor, RegEdit). Найшвидшим способом завантаження редактору є виконання наступних дій:

1. Комбінацією клавіш Win+R запустити підпрограму виконання операцій.
2. У полі вводу ввести команду «regedit» або «regedit.exe»
3. Натиснути клавішу Enter.

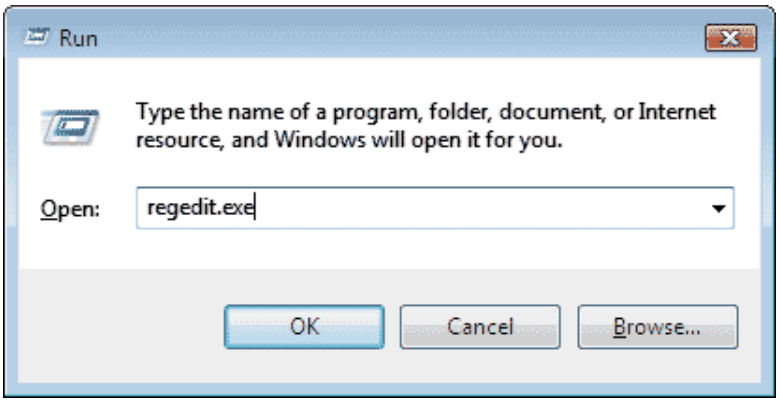


Рис. 2: Завантаження редактору реєстру

Кожен розділ (гілка) відповідає певному типу інформації про користувача, апаратне забезпечення, додатки і т.д.

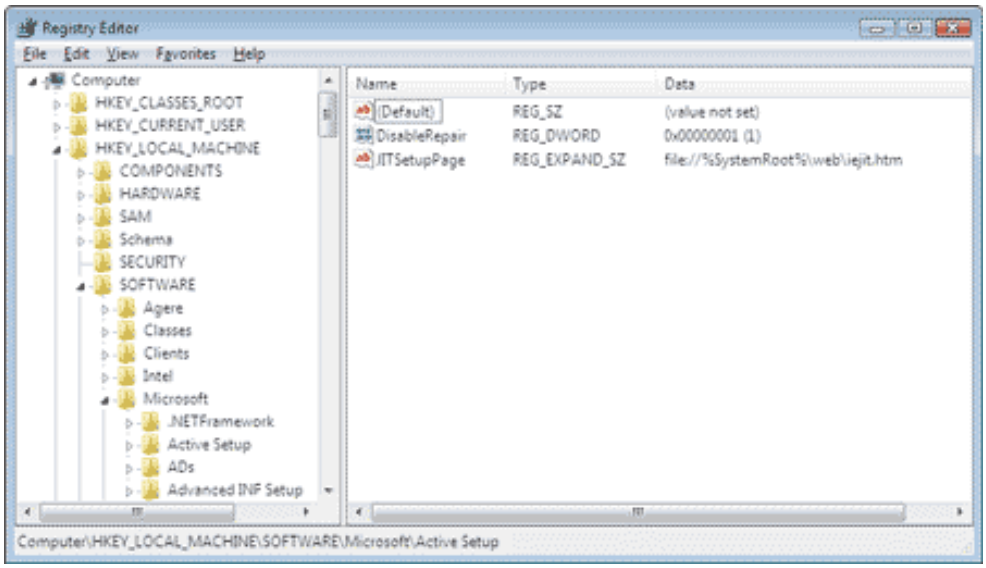


Рис. 3: Вікно редактору реєстру

Змінюючи той чи інший параметр, можна управляти роботою Windows, захистити комп'ютер від не бажаних користувачів і просто налаштовувати зовнішній вигляд.

Зокрема, в розділі `HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows\-CurrentVersion \Run` знаходиться список параметрів. Значеннями цих параметрів є імена виконуваних файлів, які завантажуються кожен раз при завантаженні системи. Додавши туди свій параметр, можна змусити систему запускати свою програму.

Для створення нового ключа реєстру необхідно перейти в той розділ, всередині якого потрібно створити новий ключ. Далі в рядку меню вибираємо Edit → New → Key (Правка → Створити → Розділ). Після цього необхідно за замовчуванням змінити ім'я створеного розділу.

Ключі в реєстрі можуть бути наступних типів:

1. `REG_BINARY` – тип довічних параметрів (Binary Value), які представляють собою набір двійкових даних, доступних для редагування тільки в шістнадцятковому форматі.
2. `REG_DWORD` – тип параметра, що має числове значення (DWORD Value), яке може задаватися в десятковому або в шістнадцятковому форматі.
3. `REG_SZ` – тип параметра, значення якого задається у вигляді текстового рядка (String Value) фіксованої довжини, даний тип параметра містить текст, який можна прочитати.
4. `REG_EXPAND_SZ` – тип параметра, значення якого задається у вигляді рядка даних змінної довжини (Expandable String Value). Цей тип даних включає імена спеціальних змінних, оброблюваних при використанні програмою або службою. Коли програма або служба читає такий рядок з реєстру – операційна система автоматично підставляє замість імен спеціальних змінних їх поточне значення.
5. `REG_MULTI_SZ` – тип параметра, значення якого задається у вигляді багаторядкового тексту (Multi-String Value). До такого типу відносяться списки та інші записи в зручному для читання форматі. Записи розділяються пробілами, комами або іншими символами.

Щоб змінити значення будь-якого параметра реєстру, необхідно знайти відповідний ключ (розділ) реєстру і виконати подвійне клацання миші на потрібному параметрі в правій частині вікна редактора реєстру. При цьому з'явиться діалогове вікно, в якому можна вказати нове значення параметра.

Для того щоб видалити який-небудь ключ реєстру, необхідно виділити його, а по-

тім натиснути на клавішу Delete (Del).

Перш ніж приступати до якихось експериментів з реєстром, необхідно створити його резервну копію, причому не повну копію реєстру, а тільки копію того розділу, який піддається модифікації. Це робиться за допомогою так званих «патчів реєстру» (registry patch), що представляють собою текстові файли з розширенням * .reg, в яких зберігаються один або кілька розділів реєстру. Патчі реєстру найчастіше також називають REG-файлами.

Створення латочок реєстру проводиться із застосуванням редактора реєстру. Для цього виділяється той розділ реєстру, який необхідно зберегти як патч. Далі в рядку меню слід вибрати File → Export ... (Файл → Експорт ...) або клацнути правою кнопкою миші на потрібному розділі реєстру і в спадаючому меню вибрати пункт Export, та зберігти файл

Після створення патчу (експортування) розділу реєстру з REG-файлом можна працювати, як із звичайним текстовим файлом, використовуючи для цього стандартні текстові редактори (наприклад, Word).

## 3 Хід роботи

Запускаємо віртуальну машину. Пропускаємо пункт про антивірусне програмне забезпечення та тестовий вірус, а також домашнє завдання, яке залежить від тестового вірусу, оскільки образ диску з необхідними файлами був відсутній у папці з завданням.

Відкриваємо редактор реєстру та переходимо до гілки `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` (рис. 4).

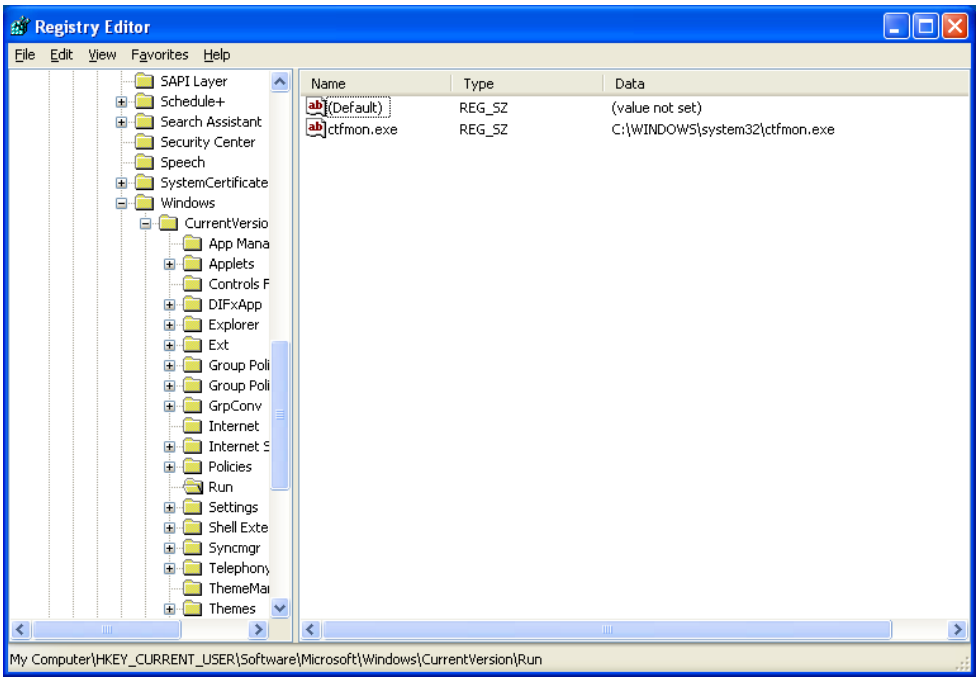


Рис. 4: Вікно редактору реєстру та вміст гілки `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

Тепер налаштуємо систему так, щоб при кожному запуску операційної системи автоматично відкривалась програма «Microsoft Paint». Для цього створимо відповідний параметр у поточній гілці реєстру операційної системи, яка відповідає саме за запуск виконуваних файлів при кожному старті системи. Щоб це зробити, у правій частині вікна викликаємо контекстне меню та вибираємо «Створити» → «Строковий параметр», задаємо для створюваного параметра ім'я «Paint». Після створення параметра редагуємо його. Для цього двічі клікаємо на створений параметр, з'являється вікно редагування. У вікно редагування в поле «Значення» вписуємо шлях до програми «Paint»:

```
C:\Windows\System32\mspaint.exe
```

Зберігаємо внесені зміни, для чого натискаємо на кнопку «ОК» (рис. 5).

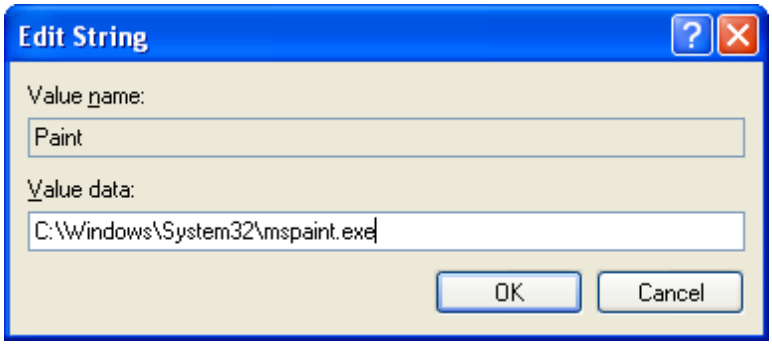


Рис. 5: Вікно редагування створеного параметра

Переконуємось, що потрібний параметр був створений у відповідній гілці реєстру з бажаним значенням (рис. 6).

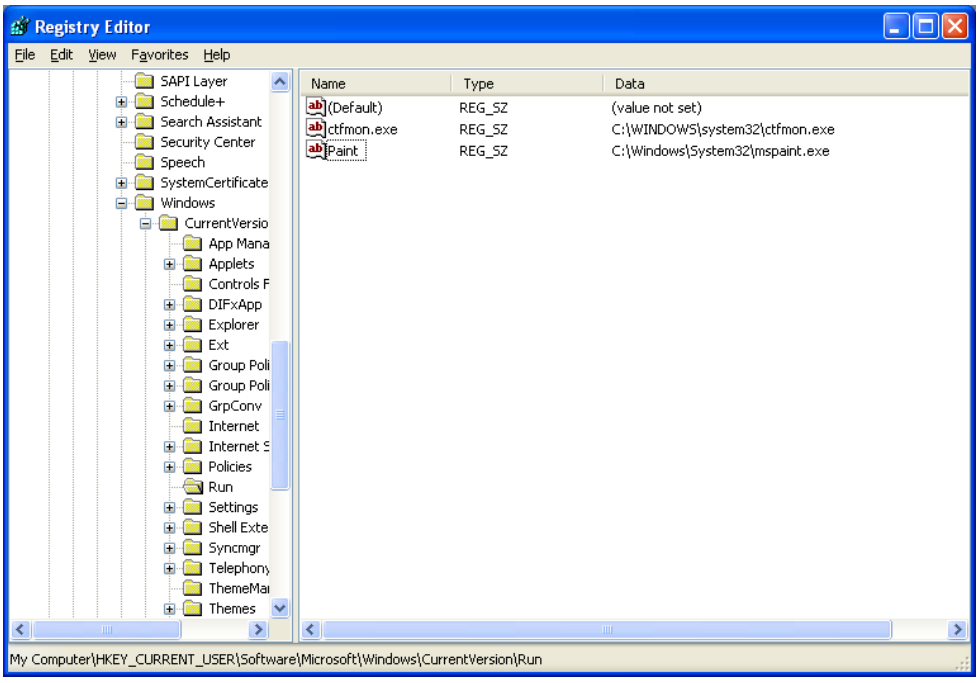


Рис. 6: Результат додавання параметра

Створений параметр тепер збережений у реєстрі операційної системи. Закриваємо редактор реєстру та переходимо до наступного кроку.

Тепер переконаємось, що в результаті внесених змін, а саме додавання необхідного параметру в реєстр операційної системи, ми досягли бажаного результату, тобто що програма «Microsoft Paint» дійсно буде запускатись при кожному старті операційної системи. Для цього виконуємо перезавантаження комп'ютера, чекаємо на повне завантаження операційної системи та спостерігаємо одержаний результат (рис. 7).

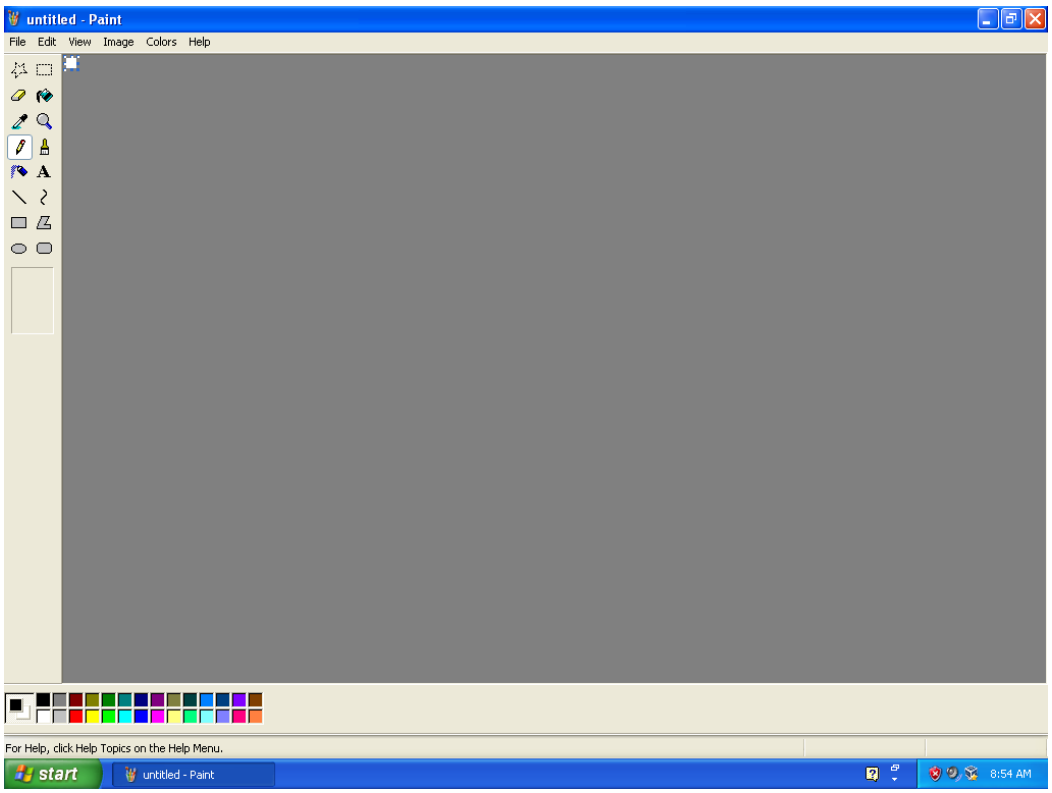


Рис. 7: Стан операційної системи одразу після запуску

Як бачимо, створення параметру «Paint» з відповідним значенням у спеціально призначеній гілці реєстру дало бажаний результат.

## 4 Висновки

Виконуючи дану лабораторну роботу, ми отримали навички адміністрування в операційній системі Windows 7.