Лабораторна робота №7

Дослідження реєстру операційної системи *Windows*

Ціль роботи: Ознайомлення з реєстром операційної системи *Windows*. Вивчення структури, параметрів та методів редагування.

1. 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 *SYSTEM*32 \ *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*).

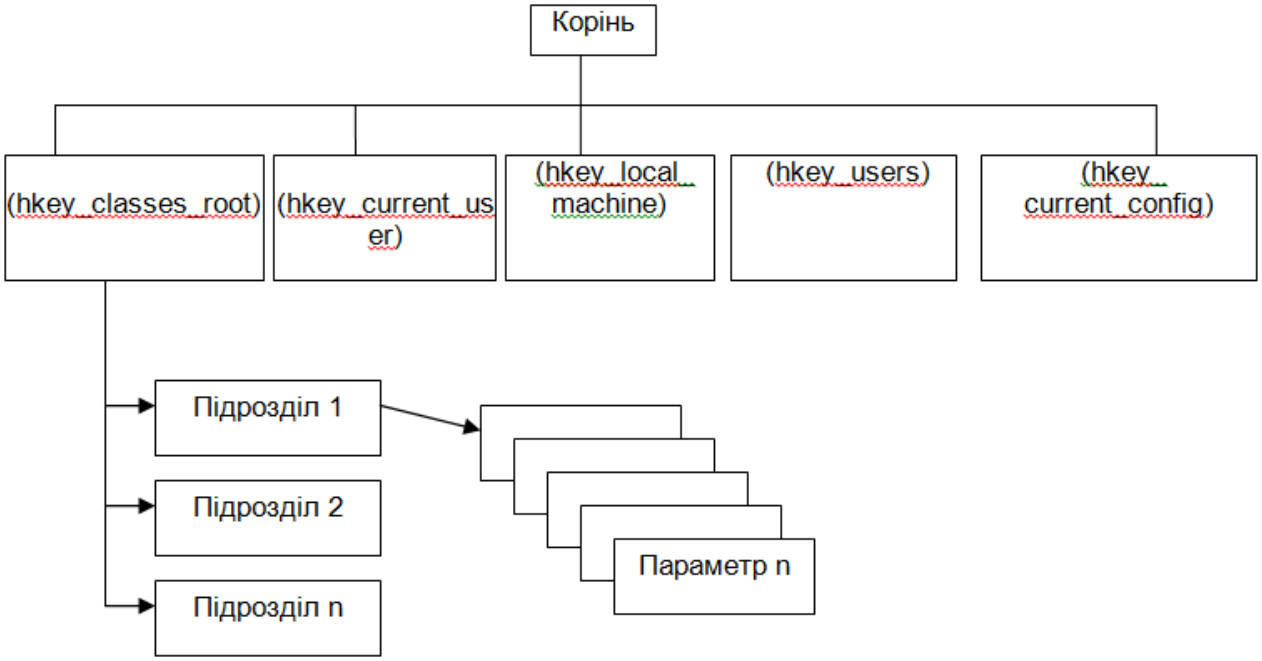

Рис. 1. Оглядовий приклад структури реєстру

Весь реєстр *Windows Vista* ділиться на п'ять основних.

Базову структуру реєстру формують саме ці розділи:

- *HKEY_CLASSES_ROOT (HKCR)*
- *HKEY_CURRENT_USER (HKCU)*
- *HKEY_LOCAL_MACHINE (HKLM)*
- *HKEY_USERS (HKU)*
- *HKEY_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:

HKLM \ Software \ Classes

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*.

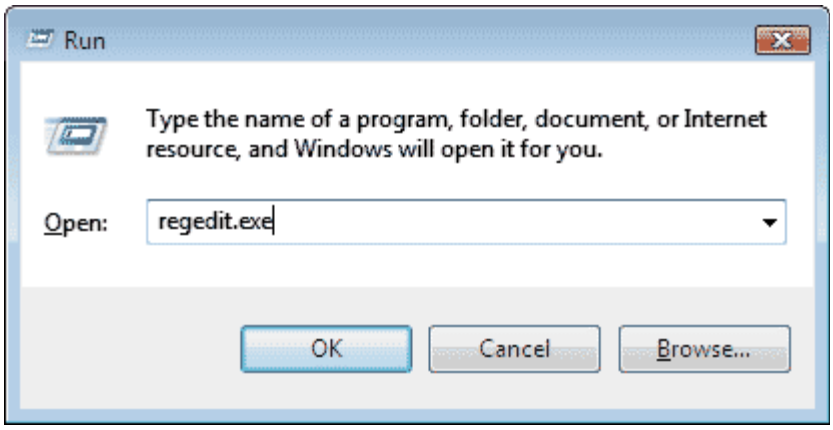

Рис. 2. Завантаження редактору реєстру

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

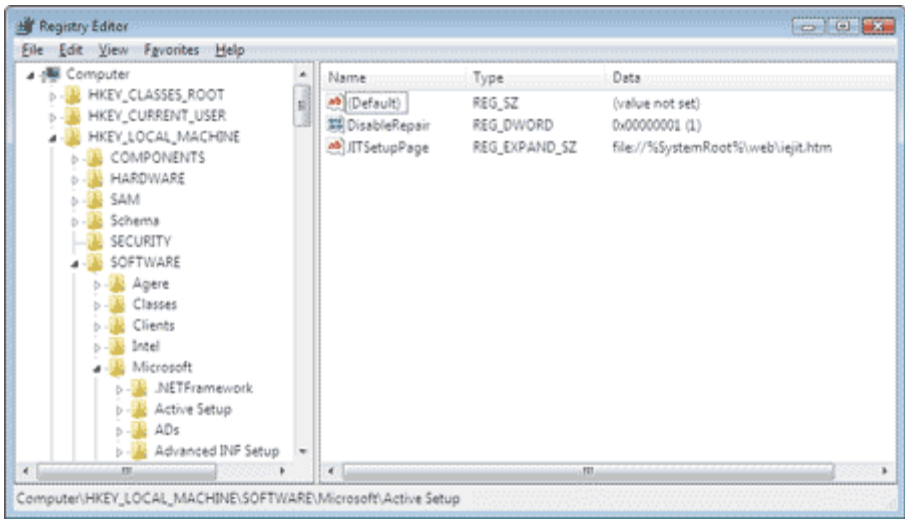

Рис. 3. Вікно редактору реєстру

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:

REG_BINARY – тип довічних параметрів (*Binary Value*), які представляють собою набір двійкових даних, доступних для редагування тільки в шістнадцятковому форматі.

REG_DWORD – тип параметра, що має числове значення (*DWORD Value*), яке може задаватися в десятковому або в шістнадцятковому форматі.

REG_SZ – тип параметра, значення якого задається у вигляді текстового рядка (*String Value*) фіксованої довжини, даний тип параметра містить текст, який можна прочитати.

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.

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 потім 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*).

Виконання роботи

1.1.Вимоги до обладнання та програмного забезпечення

Лабораторна робота виконується на ПК з використанням программ *VMware player*, *CCleaner*.

1.2. Порядок виконання роботи

1.2.1. Запустити віртуальну машину *VMware player* (рис. 1):

Рис. 1 Основне вікно програми *VMware Player*

1.2.2. Скопіювати пакет встановлення антивірусного ПО для виконання встановлення та тестовий вірус на жорсткий диск.

Для цього потрібно виконати монтування образу диску, який знаходиться в папці з лабораторною роботою. Виконання цієї операції потребує у вікні віртуальної машини перейти до налаштування пристрою *CD\DVD* (*Player-Removable Devices-CD\DVD* (*IDE*)-*Settings*…) (рис. 3):

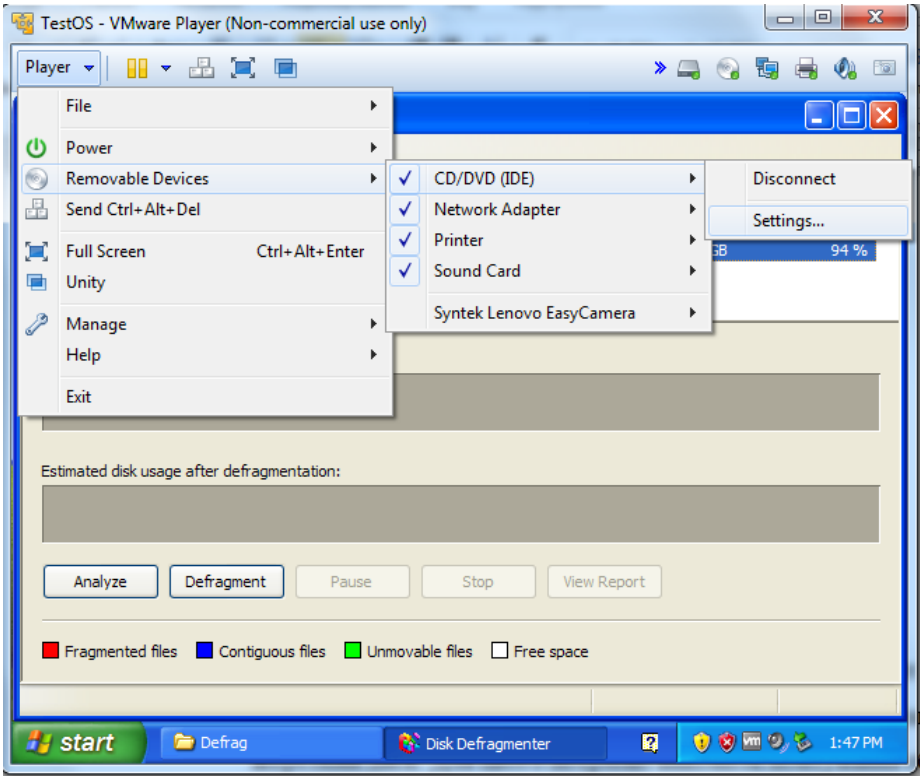

Рис. 3 Налаштування пристрою *CD\DVD Vmware*

У вікні, що з'явилось на екрані, потрібно вибрати пункт *Use ISO image file*: (рис. 4) та вказати шлях до *iso*-файлу, що знаходиться в папці з лабораторною роботою.

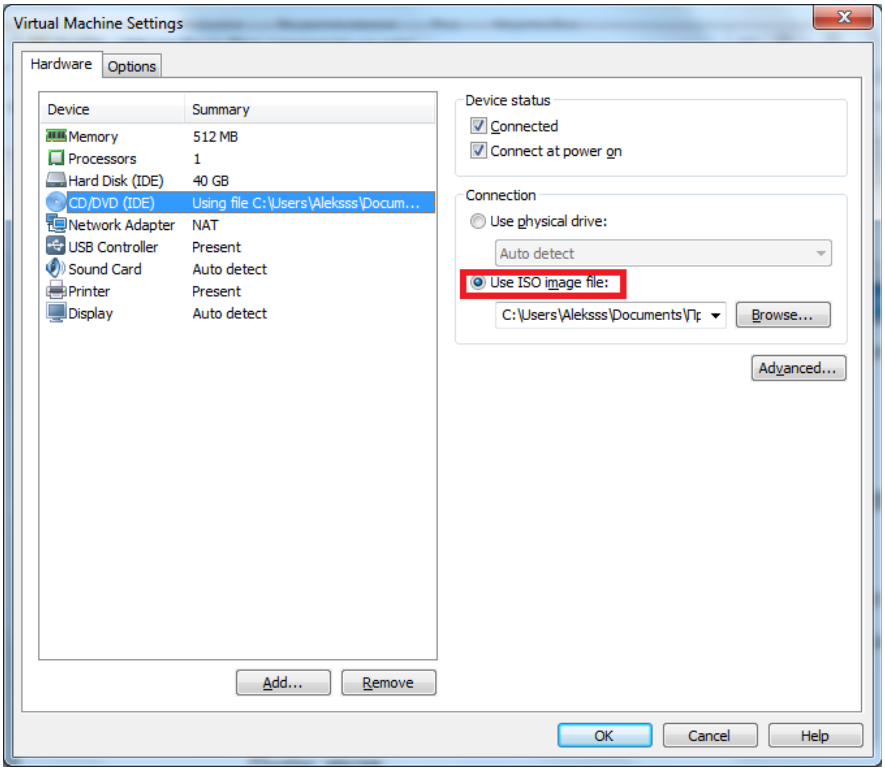

Рис. 4 Налаштування пристрою *CD\DVD VMware*

Потім потрібно натиснути кнопку *OK*. Тепер образ змонтований і ви можете отримати доступ до нього зі своєї віртуальної машини. Після відкриття диску потрібно скопіювати вміст образу на жорсткий диск віртуальної машини.

1.2.3. Відкрийте Редактор реєстру. В гілці *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*.

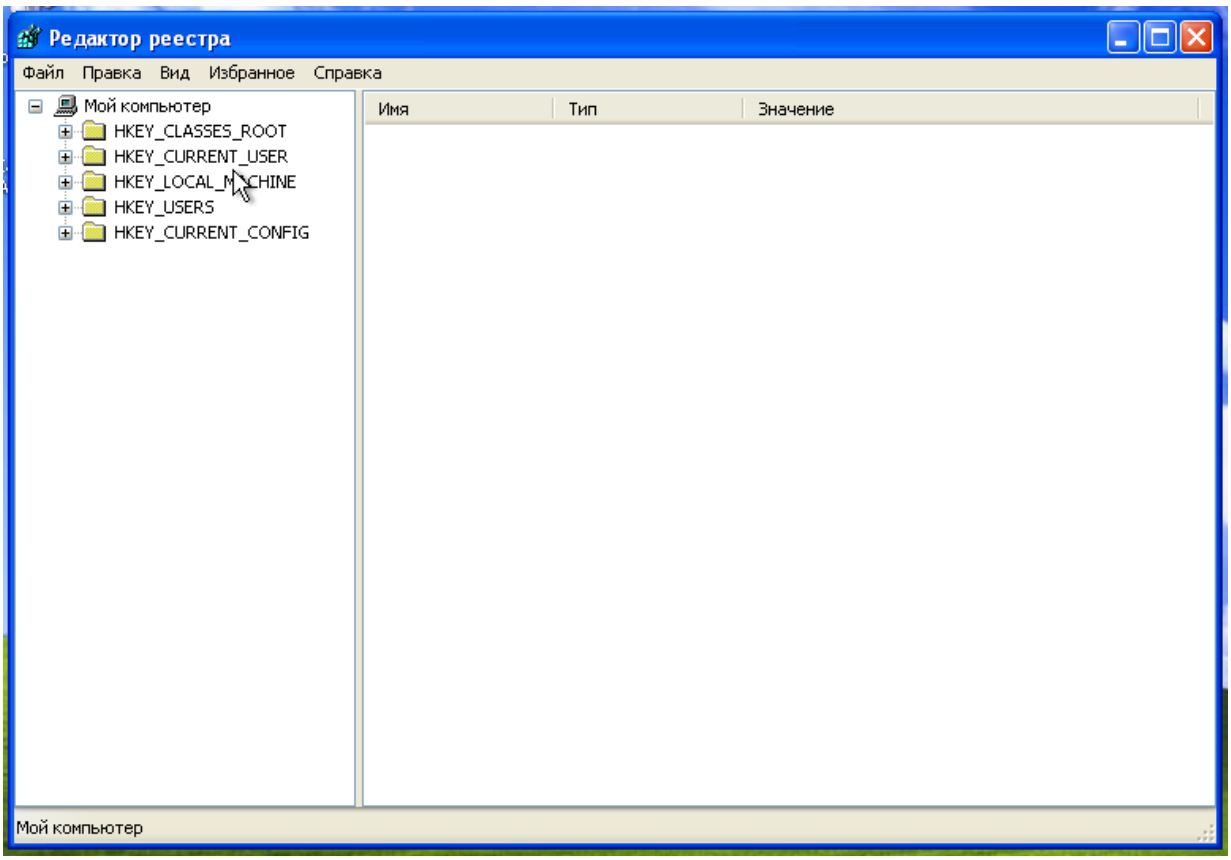

Рис. 5. Вікно редактору реєстра

1.2.4. У правій половині вікна з'явиться список ключів для даної гілки. У правій частині вікна викличте правою кнопкою миші контекстне меню і виберіть *Створити-> Строковий параметр.*

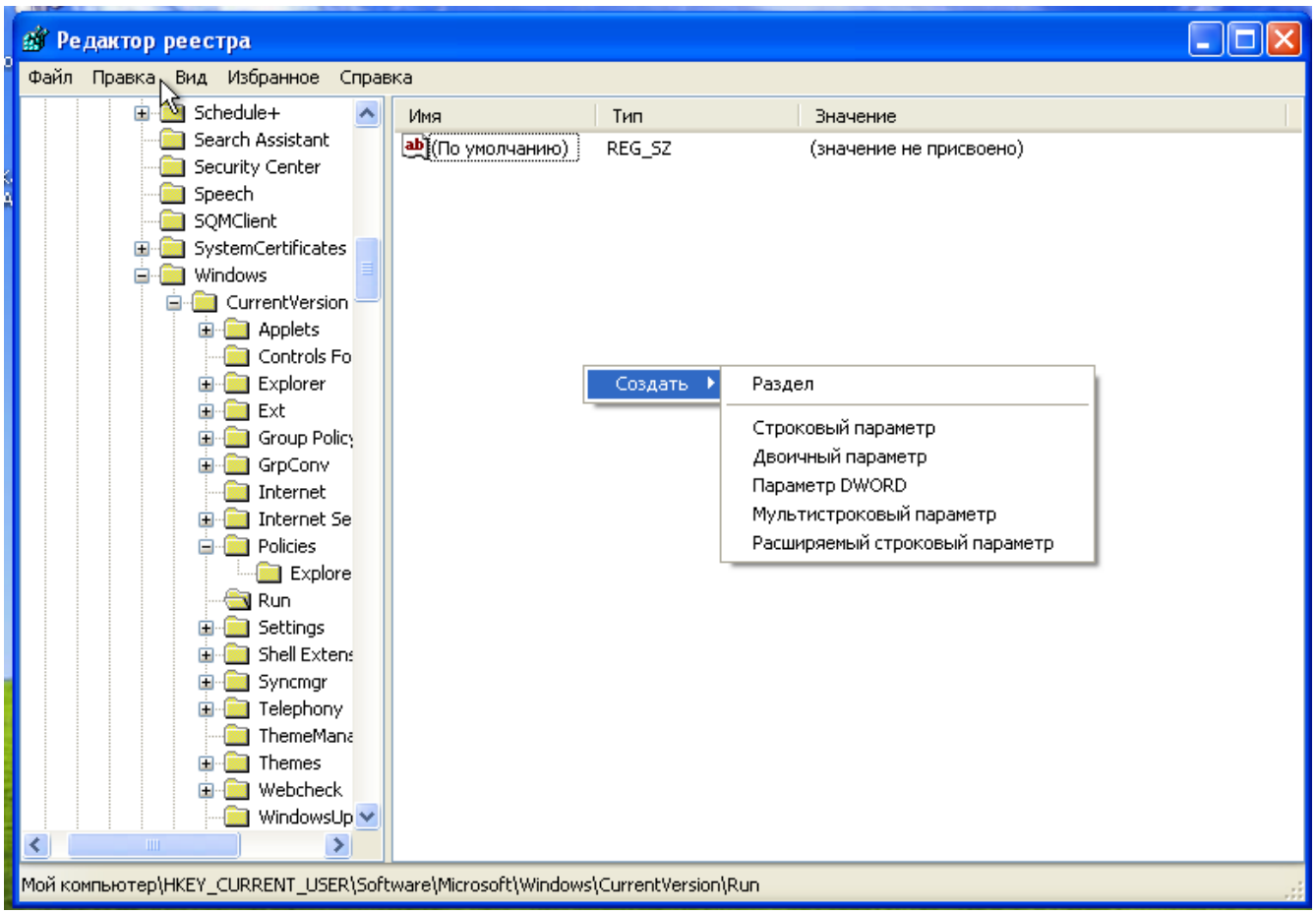

Рис. 6. Вікно редактору реєстра, створення ключа

1.2.5. Задайте ім'я для створюваного параметра *Paint*.

1.2.6. Після введення ім'я, відкрийте параметр двічі клацнувши на нього та задайте йому шлях до програми *Paint C:\WINDOWS\\System32\mspaint.exe*

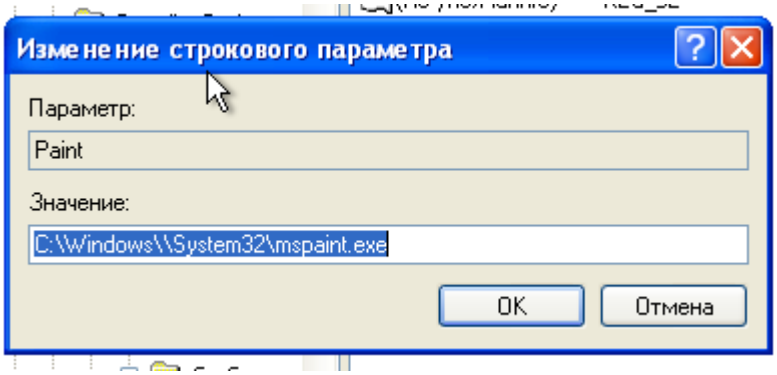

Рис. 7. Редагування ключа реєстру

1.2.7. Після введення натисніть ОК та перезавантажте віртуальну машину.

При завантаженні операційної системи відбудеться запуск програми *mspaint.exe.* Якщо програма дійсно завантажилась, то все зроблено вірно.

1.2.8. Відкрийте програму *CCleaner*. У лівому меню виберіть *Сервіс* та відкрийте вкладку *Автозавантаження*.

Тут показані програми, які запускаються або запускалися разом з *Windows*. У стовпці "*Включено*" відображений статус програми на даний момент. Якщо Для видалення програми, виберіть її та натисніть на кнопку *Видалити*. (рис. 8)

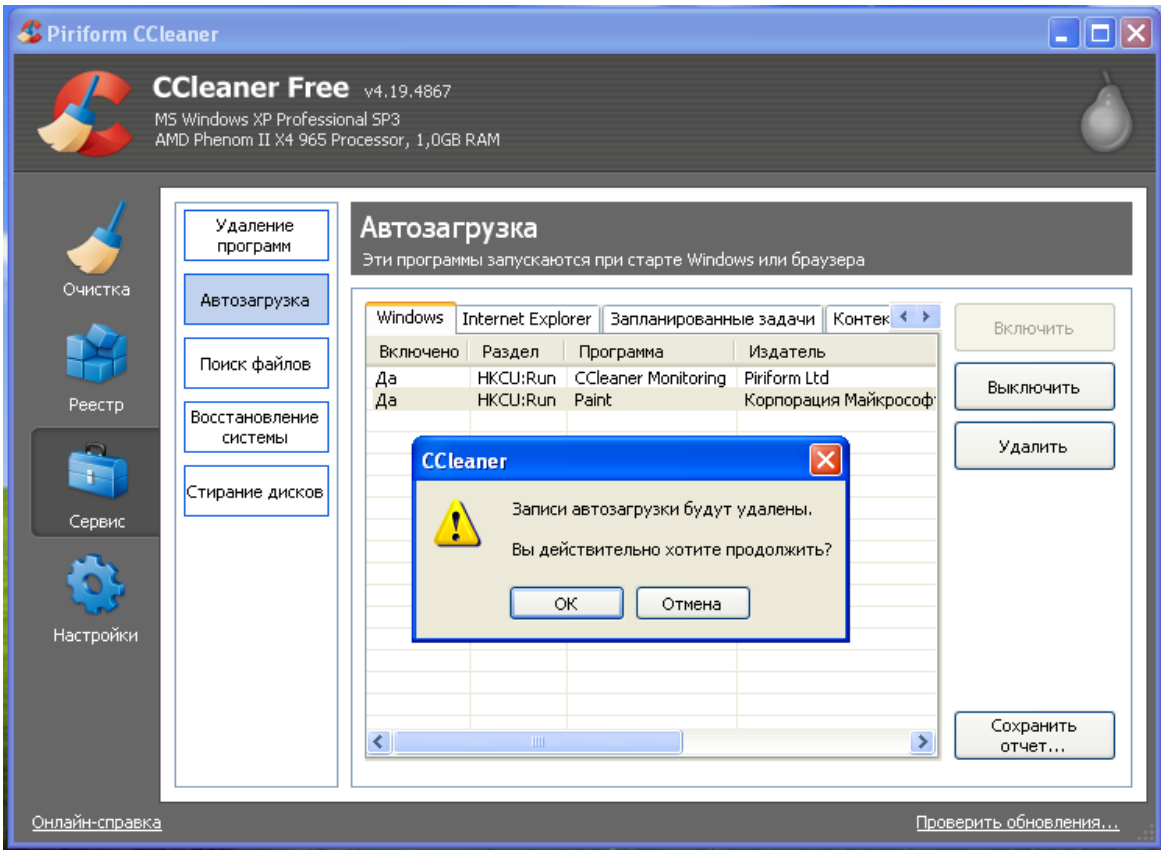

Рис. 8. Редагування ключа реєстру

1.2.9. Після видалення запису програми зі списку, перезавантажте комп’ютер та упевніться що не відбулось завантаження непотрібної програми.

2. **Домашнє завдання**.

Використовуючи набуті навички роботи з реєстром, навмисно заразіть вашу віртуальну машину «блокувальником *Windows*». Після зараження спробуйте самостійно очистити систему від блокувалника та за допомогою відмомим Вам антивірусними програмами.

3. Вимоги до вмісту і оформлення звіту

Звіт з лабораторної роботи повинен містити:

— титульний лист;

— короткі теоретичні відомості;

— опис ходу роботи;

— отримані в ході виконання роботи знімки вікон програм;

— результати виконання домашнього завдання;

— висновки.

4. Вимоги до оформлення звіту:

— сторінки А4, відступ зліва – 20, зправа – 10, зверху – 15, знизу – 15;

— шрифт *Times New Roman* 14, відступ першого рядку – 1,25, інтервал – полуторний, вирівнювання – по ширині, вирівнювання малюнків – по центру;

— сторінки нумеровані.

5. Контрольні питання

5.1. Що таке реєстр *Windows*?

5.2. Призначення реєстру?

5.3. Де і у якому виді зберігається реєстр?

5.4. Поясніть структуру реєстру, гілки, розділу, ключа. Наведіть приклад.

5.5. Який існує вбудований інструмент для редагування реєстру? Як його запустити?

5.6. У якому розділі зберігаються дані про відповідність файлів та додатків?

5.7. У якому розділі зберігаються дані про усіх користувачів та дані про активного користувача?

5.8. У якому розділі зберігаються дані про апаратну конфігурацію комп'ютера?

5.9. У якому розділі зберігаються дані про обладання комп'ютера?

5.10. Які операції можно виконувати при роботі з реєстром?

5.11. Які типи ключів можуть бути в реєстрі?

5.12. Що необхідно зробити перед редагуванням реєстру?