ЛАБОРАТОРНА РОБОТА №3

УПРАВЛІННЯ СИСТЕМНИМ РЕЄСТРОМ WINDOWS

Мета роботи: вивчити структуру ключів реєстру, типи параметрів ключів, способи редагування реєстру, отримати практичні навики роботи з редактором реєстру RegEdit.

Теоретичні відомості

Приховування значків дисків.(win_7,win_xp)

Ви можете приховувати непотрібні значки дисків у вікні комп'ютера. Наочним прикладом для цієї задачі є диск A:, що призначений для флопідисководів. Сучасні настільні комп'ютери і ноутбуки вже не комплектуються подібними дисководами, але значок A: як і раніше присутня в системі. Недосвідчений користувач може помилково клацнуть по даному значку і отримати повідомлення про помилку, яке буде збивати його з пантелику. Щоб приховати значків дисків потрібно використовувати параметр NoDrives типу
DWORD, що являється бітовою маскою. Даний параметр розташований в розділі HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer.

Значення бітової маски параметра NoDrives будуються за наступним правилом: кожній букві диска присвоюється певний біт в шістнадцятирічному значенні. Щоб приховати тільки один диск, можна вказати єдиний біт в параметрі. Якщо потрібно приховати два і більше диска, то їх значення потрібно скласти.

Ось як виглядає невелика таблиця бітів для перших дисків від A: до F::

- 0x00000001 – диск A:;
- 0x00000002 – диск B:;
- 0x00000004 – диск C:;
- 0x00000008 – диск D:;
- 0x00000010 – диск E:;
- 0x00000020 – диск F: і т. д.

Таким чином, щоб сховати значок тільки диска A:, потрібно використовувати значення 0x00000001. Якщо ми хочемо приховати диск A: і C:, то слід

використовувати значення *0x00000005* і т. д. Для приховування значків всіх дисків можна використовувати значення 0x03FFFFFF.

Зміна значків дисків (win_7)

Можна змінити вигляд значків і опис диска у вікні Комп'ютера і Провідника. для цього відкрийте розділ HKLM \ Software \ Microsoft \ Windows\ CurrentVersion \ Explorer і створіть новий підрозділ DriveIcons. Тепер в ньому необхідно створити підрозділи з літерами дисків, чиї значки та опис ви збиралися змінювати. Наступний крок - створення в підрозділах диска двох нових підрозділів: DefaultIcon і DefaultLabel.

У них потрібно змінити значення за замовчуванням. В першому випадку потрібно вказати шлях до значка, а в другому - опис диска. Наприклад, ось як виглядатимуть параметри в реєстрі для диска C::

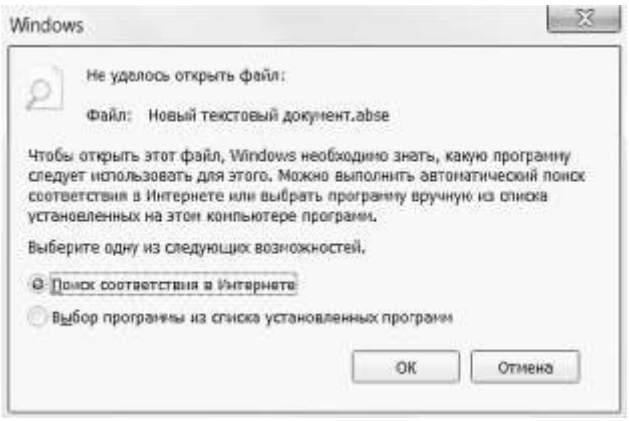
[HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ DriveIcons \ C\ DefaultIcon] @ = "explorer.exe, 8"

[HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft\ Windows \ CurrentVersion \ Explorer \ DriveIcons \ C\ DefaultLabel] @ = "Мій системний диск"

В даному випадку значок @ означає параметр по замовчуванням. На рис. ви можете бачити вікно редактора реєстру і вікно Комп'ютер, в якому видно значок диска C: зі зміненими параметрами відображення.

Діалогове вікно вибору програми (win_7)

Коли в Провіднику ви натискаєте на файлі з незареєстрованим в системі розширенням, то з'являється діалогове вікно Вибір програми, в якому вам пропонується знайти програму для обробки в Інтернеті або вибрати зі списку встановлених на вашому комп'ютері програм, яка призначена для роботи з обраним файлом. Розглянемо декілька параметрів, що дозволяють налаштувати діалогове вікно.



Не шукати в Інтернеті

Якщо системі не знайомий тип файлу, який ви намагаєтесь відкрити, то спочатку виводиться діалогове вікно ,але, з пропозицією здійснити пошук програми в інтернеті.

Якщо вибрати цей варіант, то запускається веб-служба shell.windows.com/fileassoc/0409/xml / redir.asp? Ext = rar (приклад для випадку з RAR-файлом). Можна пропустити цей крок і відразу шукати потрібну програму на своєму комп'ютері. Для цього створіть параметр NoInternetOpenWith типу DWORD зі значенням 1 у розділі HKCU \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer.

Заборона на зміну фону Робочого столу

Можна заборонити змінювати фоновий рисунок. Для цього створіть DWORD-параметр NoChangingWallpaper зі значенням 1 у розділі HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ ActiveDesktop. Посилання Фон робочого столу у вікні Персоналізація стане недоступним.

УВАГА Незважаючи на подібну заборону, користувач може змінити фон робочого столу через браузер Internet Explorer за допомогою команди Зробити фоновим малюнком.

Дозволи на запуск додатків, крім зазначених у списку

Для цього треба відкрити розділ *HKCU \ SOFTWARE \ Microsoft \ Windows \ CurrentVerson \ Policies \ Explorer* і створити там параметри *DisallowRun* типу *DWORD* зі значенням 1. Потім треба створити підрозділ з цим же ім'ям *DisallowRun* і в ньому вказати список заборонених програм у вигляді строкових параметрів. Записи в цьому підрозділі пронумеровуються, починаючи з 1, і містити рядки зі шляхами (необов'язково) та іменами пропозицій. Файли повинні бути з розширенням. Наприклад: Word.exe, Excel.exe. приклад:

«1» - calc.exe;

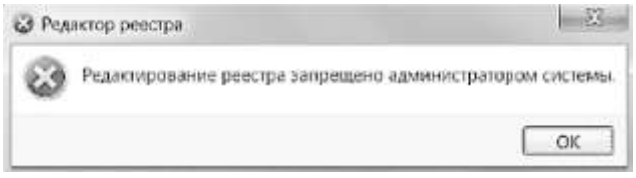
«2» - thebat.exe;

«3» - hl.exe.

Ця настройка діє на програми, які запускає процес від Windows Explorer, але не захищаючи від запуску цих програм за допомогою Менеджера завдань (Task Manager), який запускається системним процесом чи іншими процесами. Також ці програми можна запустити через командний рядок cmd.exe.

Заборона на запуск редактора реєстру

Ви можете заборонити запуск редактор реєстру. Для цього в розділі *HKCU \ SOFTWARE \ Microsoft \ Windows \ CurrentVerson \ Policies \ System* потрібно добавить параметр *DisableRegistryTools* типу *DWORD* зі значенням *1*. Запуск редактора реєстру буде забороненим, і на екрані з'явиться відповідне повідомлення. Причому, на відміну від старих версій Windows, у користувача не залишиться можливості вносити зміни за допомогою програмного забезпечення сторонніх розробників і за допомогою REG-файлів або утиліти REG.EXE. Мені довелося викликають редактор локальних групових політик.



Повідомлення при завантаженні (win_7, win_xp)

Можна налаштувати систему таким чином, щоб при завантаженні системи на екрані привітання спочатку виводилося ваше повідомлення. Для цього відкрийте розділ *HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System* (для Windows 7)повідомлення *HKLM \ Software \ Microsoft \ WindowsNT \ CurrentVersion \ Winlogon.* (Для попередніх версій) і знайдіть рядкові параметри legalnoticecaption і legalnoticetext. (для Windows 7) або LegalNoticeCaption і LegalNoticeText (для попередніх версій)

УВАГА! Не забудьте зробити резервну копію гілки реєстру або точку відновлення системи, перш ніж видаляти або модифікувати розділи реєстру!

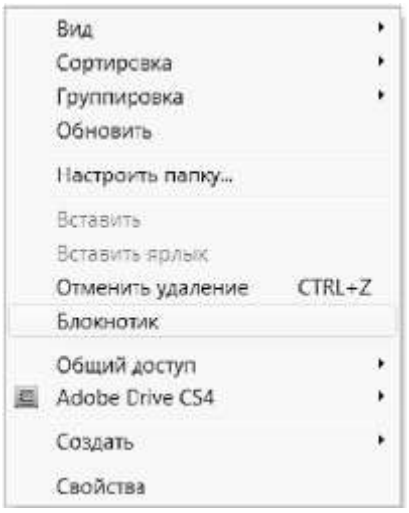
Перший параметр відповідає за заголовок повідомлення, а другий - за сам текст. Припустимо, ви введете в перший параметр текст Увага!, а в другій параметр: На комп'ютері виявлені віруси! Форматувати диск? Тепер при кожному включенні комп'ютера до появи стандартного екрану привітання ви будете бачити задане повідомлення.

Створення власних команд для контекстного меню Провідника та Робочого столу

Ми знаємо, як видаляти або редагувати деякі команди з контекстного меню Провідника і Робочого столу. Настав час навчитися створювати свої власні команди. Інформація про контекстне меню Провідника і Робочого столу зберігається в розділі реєстру *HKCR \ Directory \ Background \ Shell*. Саме звідси система дізнається, які команди потрібні, але відображаються в контекстному меню і програми, які потрібно запустити, коли користувач клацає по вибраній команді меню. Таким чином, озброївшись цими знаннями, ми зможемо самі створювати потрібні нам команди. Для додавання нової команди в контекстне меню, досить створити в розділі *HKCR \ Directory \ Background \ Shell* новий підрозділ. Припустимо, ми хочемо, щоб в меню з'явилася команда, запускаються стандартний Блокнот. Створюємо підрозділ notepad і відразу можемо перевірити і переконатися, що в контекстному меню Робочого столу з'явилася одноіменна команда.

Природно, така команда не дуже нас влаштовує, і ми хочемо задати власний текст, наприклад Блокнотик. Для цього редагуємо параметр за замовчуванням створення підрозділу і записуємо для нього нове значення, яке ми хочемо бачити, наприклад, слово «Блокнотик»

Перевіряємо і переконуємося, що в контекстному меню з'явилася команда Блокнотик. Пункт меню ми додали, але клацання по ньому ще немає до чого корисного не призводить. Для того щоб новий пункт меню не тільки відображався, а й працював, нам знадобиться настроїти ще деякі параметри.



Підрозділ notepad може містити в собі інші підрозділи і різні параметри строкового типу. Спочатку розглянемо параметри. Можна використовувати такі параметри:

• *MUIVerb* - значення даного параметра замінює собою значення параметра за замовчуванням, тобто ми можемо в ньому задати ім'я для команди в меню.

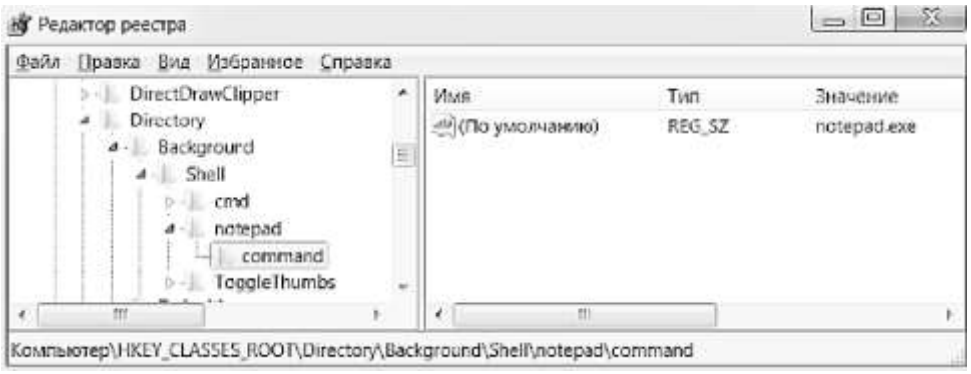
• *Extended* - наявність даного параметра без значення каже системі про те, що команда може відображатися тільки при натисканні клавіші Shift. Ви можете подивитися на підрозділ *HKCR \ Directory \ Background \ shell \ cmd*, в якому

міститься такий параметр. Тому, якщо тримати натиснутою клавішу *Shift*, в контекстному меню з'явиться команда Відкрити вікно команд.

• *LegacyDisable* - присутність даного параметра забороняє відображення в контекстному меню створеної команди. Правда, тоді не зрозуміло, навіщо взагалі створювати команду, якщо її не потрібно виводити на екран.

• *ProgrammaticAccessOnly* - присутність даного параметра так само забороняє відображення в контекстному меню створюваної команди, дозволяючи тільки програмний доступ до неї.

• *NoWorkingDirectory* - наявність даного параметру говорить про те, що при роботі програми (якщо команда контекстного меню запускає програму) не потрібно вказувати робочий каталог програми. Тепер перейдемо до підрозділів. Перш за все, потрібно створити підрозділ *command*. параметр по замовчуванням даного підрозділу повинен містити в собі команду, яка буде виконуватися при виборі відповідного елемента контекстного меню. В нашому випадку потрібно прописати команду notepad.exe



Установка і видалення програм(win_xp).

Як відомо, несанкціоноване видалення або некваліфікована установка тих чи інших програм можуть призвести до досить неприємним останнім наслідком. Щоб уникнути подібних ситуацій, можна за допомогою системного рєєстра закрити доступ до виконання команди Панель керування *Установка та видалення програм*. Для цього необхідно в розділі реєстру *HKEY_CURRENT_USER \ Sof tware \ Microsoft Windows \ CurrentVersion \ Policies* створити підрозділ *Uninstall*, включити в нього параметр *NoAddRemovePrograms* типу *DWORD*, якому слід

присвоїти значення *1.* Відповідний REG-файл наведено нижче (розташування файлу на диску- Файли реестра \ *Інтерфейс* \ *InterNoAddRemProgr*. ред).

Windows Registry Editor Version 5.00 ..: •, *>.

[HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Uninstall]

"NoAddRemovePrograms" = dword: 00000001

Тепер, при виконанні команди Панель керування • Установка й видалення програм, на екрані з'явиться повідомлення

Екран (win_xp) У даному розділі розглянемо, яким чином, використовуючи можливості системного реєстру, можна змінювати режим роботи і подання інформації у вікні Властивості: Екран, що відкривається через Пуск • Панель керування • Екран. Зазначимо, що в деяких випадках буває корисно взагалі заборонити користувачам роботу в цьому вікні. Для цього необхідно створити параметр *NoDispCPL* типу *DWORD* в розділі реєстру *HKEY_CURRENT_USER \ Sof tware \ Microsof t \ Windows \ CurrentVersion \ Policies \ System* і привласнити йому значення *1* (якщо підрозділ System по зазначеному шляху відсутня, то його потрібно створити самостійно). У цьому випадку REG-файл буде виглядати так (розташування файлу на диску - Файли реєстру *VHHTepiJieiicMnterNoDispCPL.reg*): Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System]

"NoDispCPL" = dword: 00000001

Тепер при спробі виконання команди Пуск • Панель керування • Екран на екрані з'явиться повідомлення про те, що системний адміністратор заблокував роботу в цьому режимі (рис. 2.81). Відзначимо, що аналогічне повідомлення буде виведено і при активізації функції Властивості, яка міститься в контекстному меню Робочого столу.

Робочий стіл (win_xp)

Для видалення вкладки Робочий стіл з вікна Властивості: Екран необхідно в розділі реєстру

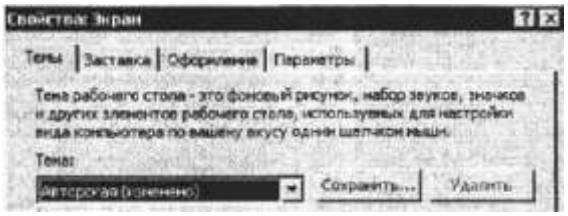
HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \Policies \ System

створити параметр *NoDispBackgroundPage* типу *DWORD* і привласнити йому значення 1.

[HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System]

"NoDispBackgroundPage" = dword: 00000001

В результаті проведених змін вкладка Робочий стіл буде видалена з вікна редагування властивостей екрану

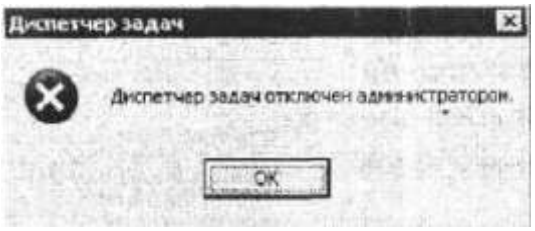


Диспетчер завдань(win_xp) Як відомо, натисканням комбінації клавіш Ctrl + Alt + Delete на екран виводиться вікно Диспетчер завдань Windows. Іноді буває корисно заборонити користувачам роботув даному вікні - наприклад, щоб виключити некваліфіковане втручання. Для цього в розділі *HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System* слід створити параметр DisableTaskMgr типу DWORD і привласнити йому значення 1 (якщо підрозділ System відсутній з зазначеному шляху, то його слід створити самостійно).

[HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ System]

"DisableTaskMgr" = dword: 00000001

Тепер при натисканні комбінації клавіш Ctrl + Alt + Delete па екрані відобразиться наступне повідомлення



Автозапуск компакт-дисків (win_xp)

Не всім користувачам подобається режим автозапуску компакт-дисків, установленний за замовчуванням в системі. За допомогою реєстру можна відключити цю функцію. Для цього необхідно в розділі реєстру HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Cdrom привласнити параметру AutoRun значення 0.

[HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Cdrom]

"AutoRun" = dword: 00000000

Після внесення до реєстру зазначених змін режим автозапуску компактдисків буде вимкнено. Для його включення необхідно параметру AutoRun присвоїти значення 1. Всі зміни вступають в силу після перезавантаження комп'ютера.

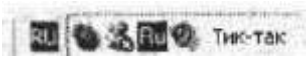
Годинник (win_xp)

Існує кілька цікавих трюків, що дозволяють змінювати режими відображения годин, які розташовані в правому нижньому кутку екрана.

У розділі реєстру *HKEY_CURRENT_USER \ Control Panel \ I nternational* сотримається строковий параметр sTimeFormat, якому за замовчуванням присвоєно значення *H: mm: ss*. Це значення включає знайомий нам формат відображення годин. Якщо ж параметру привласнити будь-яке інше значення, то воно буде відображатися на екрані замість годинника

[*HKEY_CURRENT_USER \ Control PanelMnternational] "sTimeFormat" = "Тік-так"*

Після внесення зазначених змін комп'ютер слід перезавантажити; в результаті замість звичного часу в правому нижньому кутку монітора відображається введене значення



Існують також програми для роботи з реєстром, в які вже вбудовані більшість з вище описаних можливостей. Нижче будуть наведені одні з них:

1. Vit Registry Fix

Призначена для очищення реєстру програма має такі особливості:

- Наявність в комплекті додаткових утиліт. Вони допоможуть не тільки уникнути помилок в реєстрі, а й оптимізувати файлову систему, автозавантаження, видалення встановлених програм в майбутньому, провести чистку жорсткого диску від тимчасових і непотрібних файлів;
- Можливість автоматично визначити і видалити до 50 видів помилок в реєстрі, що істотно покращує роботу комп'ютера;
- Надає можливість створення резервних копій перед видаленням;
- Очищає робочий стіл від ярликів з невірно вказаними шляхами;

2. Reg Organizer

Якщо для попередньої програми основним призначенням була чистка реєстрів, то у Reg Organizer налаштування оптимізації значно розширені. Це не просто програма очищення, а й оптимізатор взаємодії з ПК. Вона вам підійде, якщо потрібно не тільки позбавити Windows реєстр від мотлоху, залишків і помилкових даних, але і виконати ряд інших дій.

Програма чищення дозволяє:

- Дефрагментувати і стискати системні файли;
- Завдяки технології Full Uninstall видаляє будь-яке програмне забезпечення без слідів, чого неможливо досягти при звичайній деінсталяції;
- Знаходить ключі, невидимі для інших утиліт;
- В якості додаткової можливості дозволяє налаштувати Windows під користувача і контролювати роботу додатків в автозавантаженні;
- Інструмент призначений для 32- і 64-рарзрядних операційних систем Windows XP, Windows 7, Windows 10.

3. Process Monitor

Можливості:

- відстеження запуску та завершення роботи процесів і потоків, включаючи інформацію про код завершення;
- відстеження завантаження образів (бібліотек DLL і драйверів пристроїв, що працюють в режимі ядра);
- більше зібраних даних про параметри операцій введення і виведення;
- нешкідливі фільтри дозволяють встановлювати фільтри, які не будуть призводити до втрати даних;
- збір стеків потоків для кожної операції дозволяє в більшості випадків визначити вихідну причину виконання операції;
- достовірний збір інформації про процеси, включаючи шлях до образу процесу, командний рядок, а також ID користувача і сесії;
- настроюються і переміщувані колонки для кожного властивості події;
- фільтри можна встановити на будь-яке поле з даними, включаючи поля, які не є колонками;
- вдосконалена архітектура записи журналів розширює можливості програми до десятків мільйонів зареєстрованих подій і гігабайтів записаних даних про події;
- дерево процесів відображає відносини між усіма процесами, перерахованими в відомостях трасування;
- основний формат журналу зберігає всі дані, щоб їх можна було завантажити в іншому екземплярі програми Process Monitor;
- підказки до процесів для простого перегляду інформації про спосіб процесу;
- детальні підказки дозволяють отримати зручний доступ до форматованим даними, які не поміщаються в колонці;
- запис в журнал всіх операцій під час завантаження системи.

Хід роботи

1. Приховати іконки на робочому столі за допомогою редактора реєстру.
2. Приховати диски за допомогою редактора реєстру.
3. Змінити іконки для будь яких системних піктограм за допомогою редактора реєстру.
4. За результатами роботи оформити звіт. У звіті необхідно навести знімки екрану, що будуть підтверджувати виконані завдання.

Контрольні питання:

1) Яка інформація не зберігається в системному реєстрі
2) Яким чином доступний реєстр
3) Де розміщується спеціальний редактор REGEDIT.EXE
4) Яка кількість розділів в системному реєстрі
5) Кому за замовченням дозволено редагування реєстру
6) Скільки є основних розділів реєстру у WINDOWS 2k
7) Яка інформація не містяться в розділах реєстру
8) В якому вигляді зберігається інформація в системному реєстрі 9) Що з перерахованого не відноситься до атрибутів параметра реєстру
10) Що не підлягає корегуванню, видаленню в системному реєстрі
11) Які з перерахованих об’єктів не можна приховати за допомогою реєстру
12) Що необхідно створити для автоматичного редагування реєстру
13) Яка команда дозволяє запустити перегляд системних файлів
14) Які з перерахованих файлів не відносяться до системних
15) Які з перерахованих файлів не запускає команда перегляду системних файлів в Windows XP
16) В якому розділу реєстру зберігаються поточні настроювання таких параметрів, як здатність дисплея або гарнітура шрифту
17) В якому розділу реєстру зберігається інформація про змінні середовища, принтера і конфігураційних додатків для користувача, зареєстрованого в системі в даний момент
18) В якому розділу реєстру зберігається інформація про налаштування конфігурацій користувача
19) В якому розділу реєстру зберігається інформація про устаткування комп'ютера 20) В якому розділу реєстру зберігається інформація про встановлене програмне забезпечення
21) В якому розділу реєстру міститься інформація про зареєстровані типи файлів

22) Які з перерахованих типів не може мати параметр реєстру
23) Який тип даних має параметр NoDrives
24) Які з перерахованих об’єктів не налаежать до системних об'єктів робочого столу
25) В яких файлах розміщена інформація системного реєстру WINDOWS 2k
26) Де розміщений файл SAM у WINDOWS 2k 27) Де розміщений файл SOFTWARE у WINDOWS 2k 28) Де розміщений файл SYSTEM WINDOWS 2k
29) Де розміщений файл SECURITY WINDOWS 2k
30) Де розміщений файл DEFAULT WINDOWS 2k
31) Які з перерахованих файлів не містять інформацію реєстру WINDOWS 2k
32) Який з перерахованих файлів належить до WINDOWS 2k
33) Включити диски –

34) Які диски включає значення параметра NoDrives –