

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
імені ТАРАСА ШЕВЧЕНКА**



**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №3**

**3 курсу**

**«Безпека мереж і комп'ютерних систем»**

*студента 2 курсу  
групи ПП-22  
спеціальності 122 «Комп'ютерні науки»  
ОП «Прикладне програмування»  
Шевлюк Вікторії Віталіївни*

*Перевірів:  
д.т.н, професор  
Сайко В. Г.*

**Київ 2022**

## **Тема:** Моніторинг завантаження програм в середовищі ОС WINDOWS

**Мета роботи:** Дослідити принципи налаштування автоматичного завантаження програм

### **Завдання:**

1. Увійдіть в операційній системі з правами адміністратора.
2. Виконайте збереження поточного вмісту системного реєстру шляхом експорту всіх його гілок в файл.
3. Перегляньте по черзі всі гілки реєстру, що відносяться до автозавантаження і зробіть скріншоти їх вмісту (якщо гілка в реєстрі присутня).
4. Перегляньте вміст всіх папок автозавантаження і також зробіть скріншоти їх вмісту.
5. Відповідно до наведеного порядку автозавантаження комп'ютера побудуйте на підставі отриманих даних перелік додатків в порядку їх завантаження в операційній системі.
6. Створіть свою власну папку для автозавантаження і задайте новий шлях до неї. Помістіть в неї ярлик будь-якої програми і перевірте результат після перезавантаження комп'ютера. Відновіть папку за замовчуванням.
7. Створіть задачу на автоматичне завантаження файлу на свій вибір за допомогою Планувальника завдань.
8. Дослідіть перелік програм, що завантажуються автоматично за допомогою системної утиліти msinfo32.exe. Порівняйте перелік програм, що автоматично завантажуються,

отриманий за допомогою даної утиліти, з тим, що отриманий в пункті 4. Відзначте неузгодженості.

9. Проведіть аналогічні дослідження за допомогою системної утиліти msconfig.exe. Також порівняйте перелік програм, що завантажуються автоматично з тим, що отриманий в пункті 4 і відзначте неузгодженість.

10. Визначте, які з програм, що завантажуються автоматично не є критично важливими для роботи операційної системи. З подібних програм виберіть дві, які виключіть з переліку за допомогою зняття позначки у вікні "Автозавантаження" утиліти msconfig.exe.

11. Перезавантажте комп'ютер і переконайтеся в працездатності операційної системи без виключених з автозавантаження програм. Перевірте формування підрозділів для тимчасово виключених з автозавантаження програм ( "Run-") і наявність параметрів в цих підрозділі: HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run.

12. Зробіть скріншоти вмісту зазначених підрозділів

13. Проведіть дослідження автозавантаження комп'ютерів за допомогою програм, які додаються до лабораторної роботи:

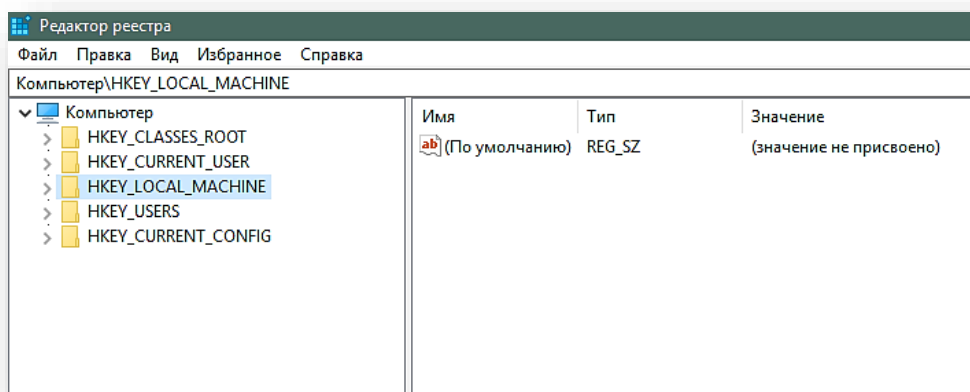
- Autoruns;
- Starter (попередньо проінсталювати);
- Startup extractor;
- Ainfo startup manager setup.

14. Скасуйте автозавантаження програми, виконану в пункті 13, відновивши первісний стан реєстру.

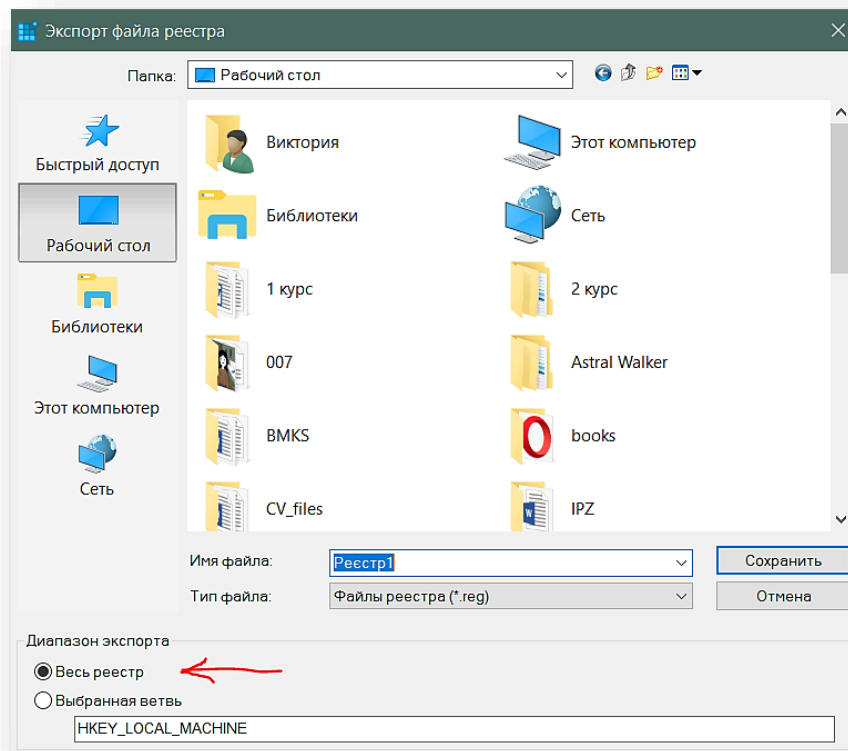
15. Складіть протокол, в якому містяться скріншоти виконання всіх завдань. Результати і висновками пред'явіть викладачеві.

### Хід роботи:

Почнемо з того, що увійдемо в систему з правами адміністратора. У мене це відбувається автоматично. Тепер нам потрібно зберегти поточний стан системного реєстру. Для цього відкриваємо редактор реєстру:



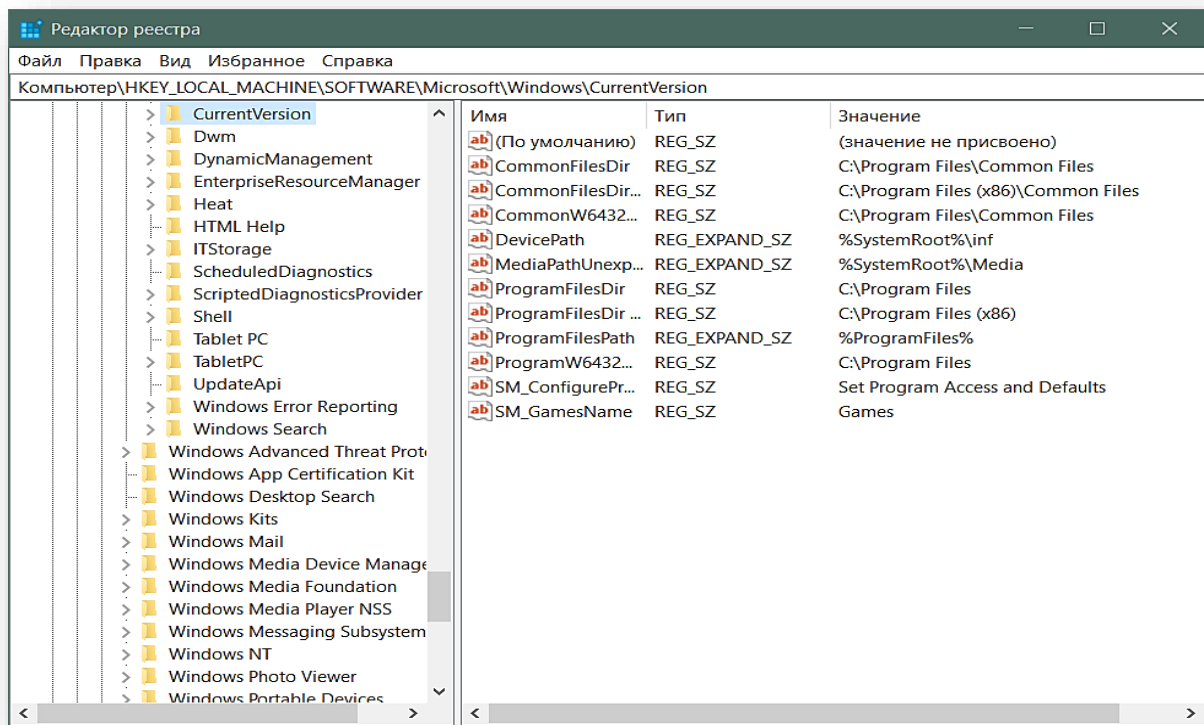
Натискаємо «Файл» і обираємо у меню «Експорт». Далі ми можемо обрати, експортувати одну папку чи весь реєстр, обираємо другий пункт і зберігаємо на робочий стіл:



Переходимо назад до реєстру. Нам потрібно переглянути усі гілки, що відповідають за автозавантаження та зафіксувати їх вміст скріншотами.

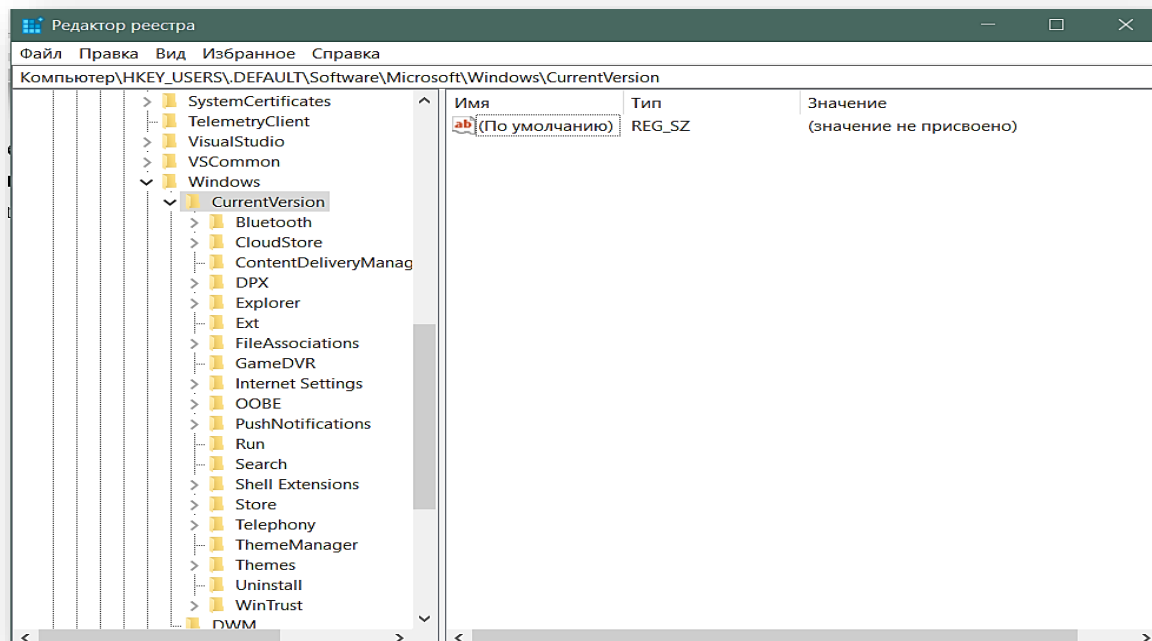
Спочатку перевіряємо вміст гілки:

Комп'ютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion



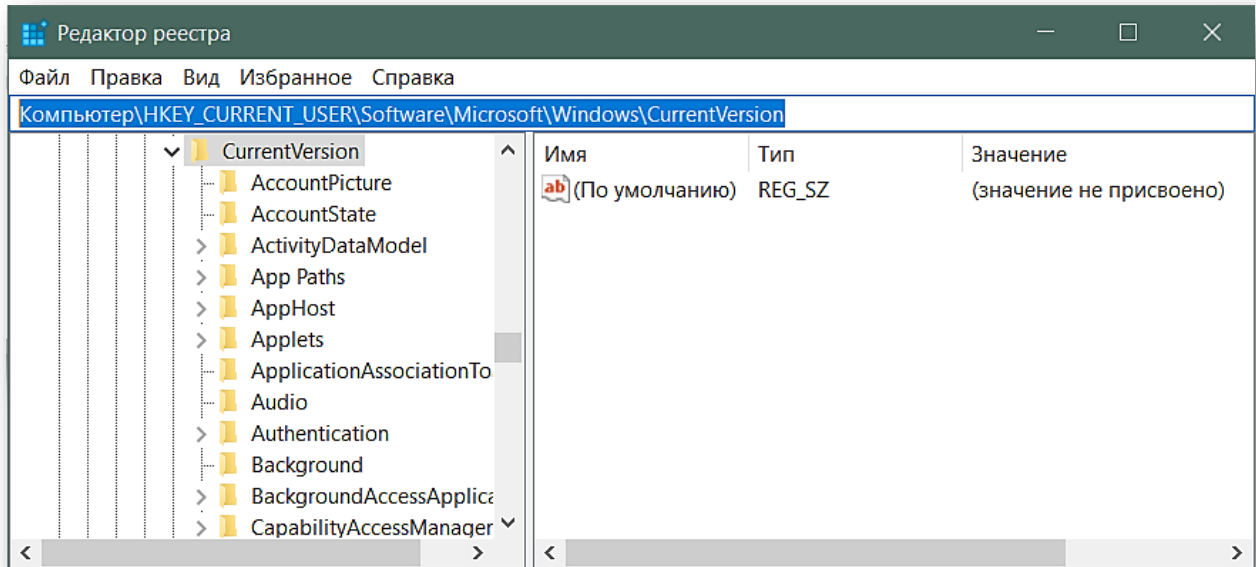
Тепер

Компьютер\HKEY\_USERS\.\DEFAULT\Software\Microsoft\Windows\CurrentVersion

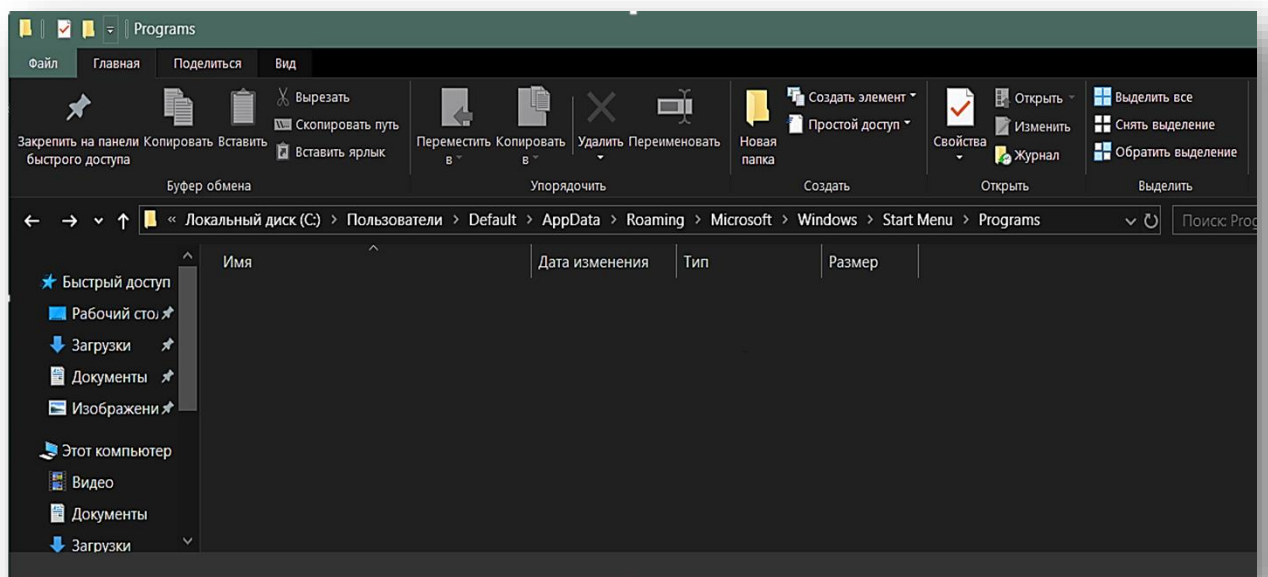


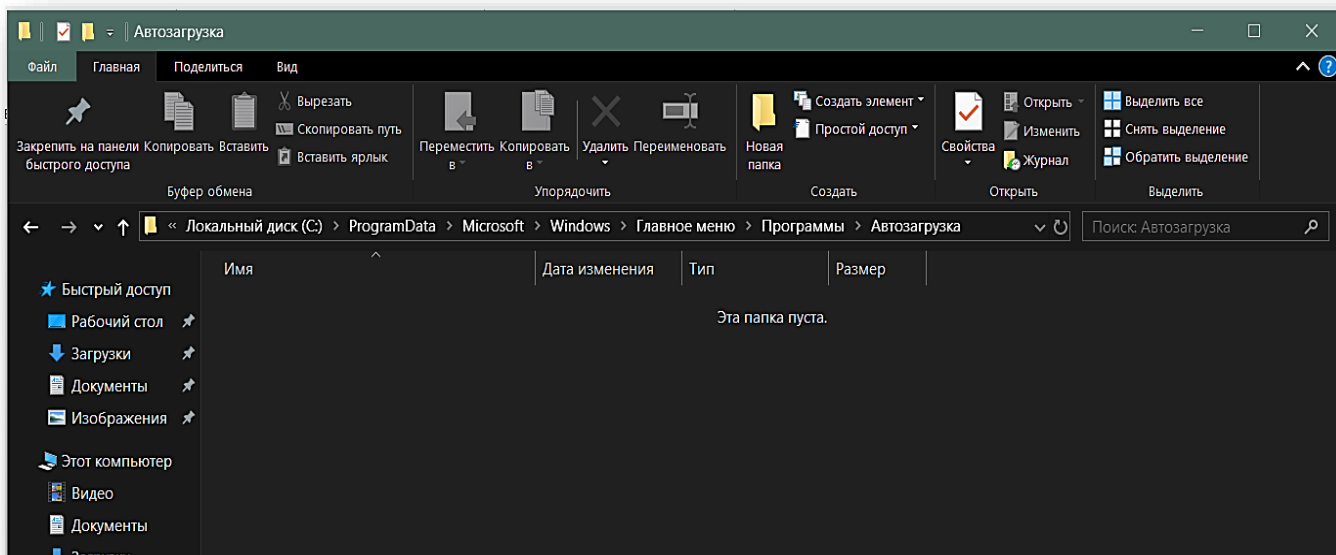
Далі:

Компьютер\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\  
CurrentVersion



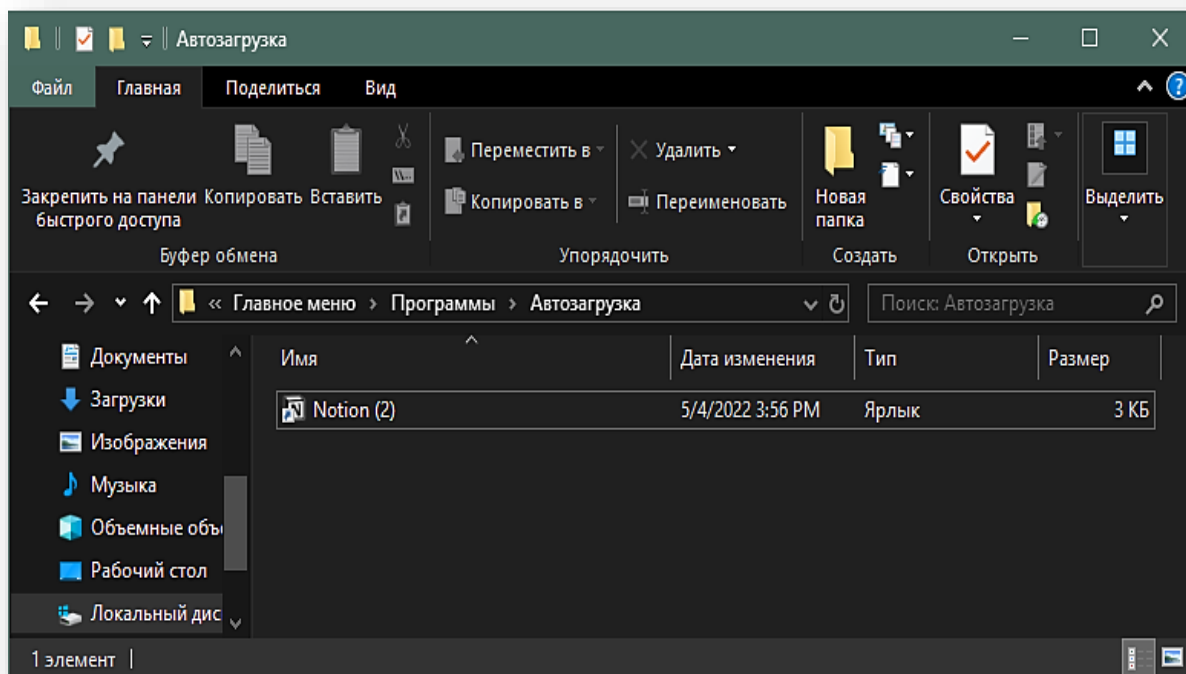
Тепер переглянемо папки автозавантаження та зафіксуємо їх  
вміст скріншотами. Для цього використаємо Провідник:





Переглянувши вміст цих папок, можемо побачити що вони пусті. Це свідчить про те, що ні одна програма не запускається автоматично при увімкненні комп'ютера.

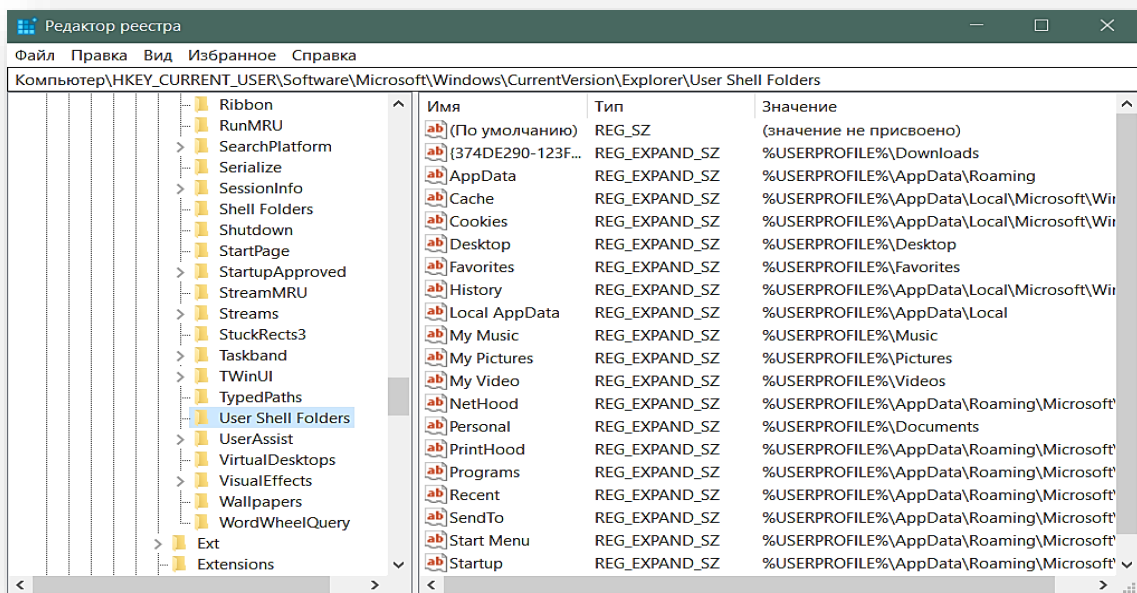
Тепер створимо свою папку для автозавантаження та додамо до неї ярлик програми, яку ми хочемо завантажувати одразу після ввімкнення пристрою:



Для зміни папки автозавантаження в реєстрі потрібно перейти шляхом:

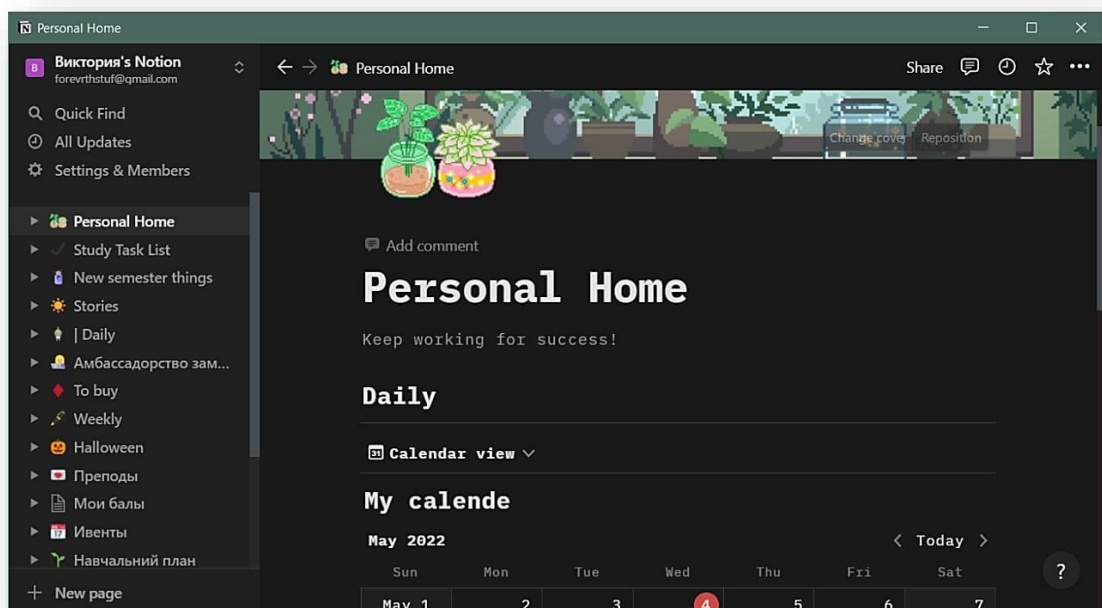


HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ User Shell Folders.

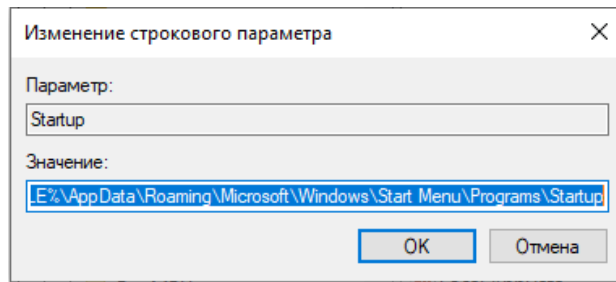


Тепер обираємо «Startup» та замінюємо у ньому шлях до нашої створеної папки.

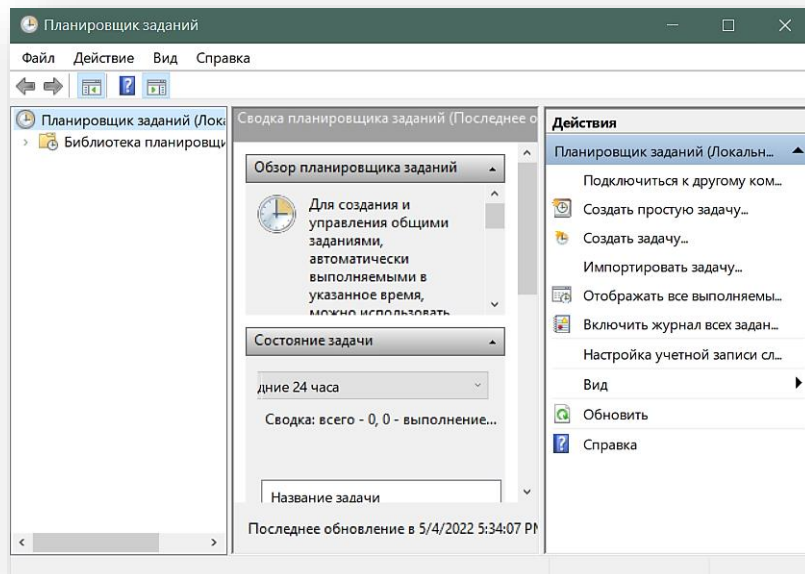
Після перезавантаження комп'ютера запустилась програма, яку я додала до папки автозавантажень:



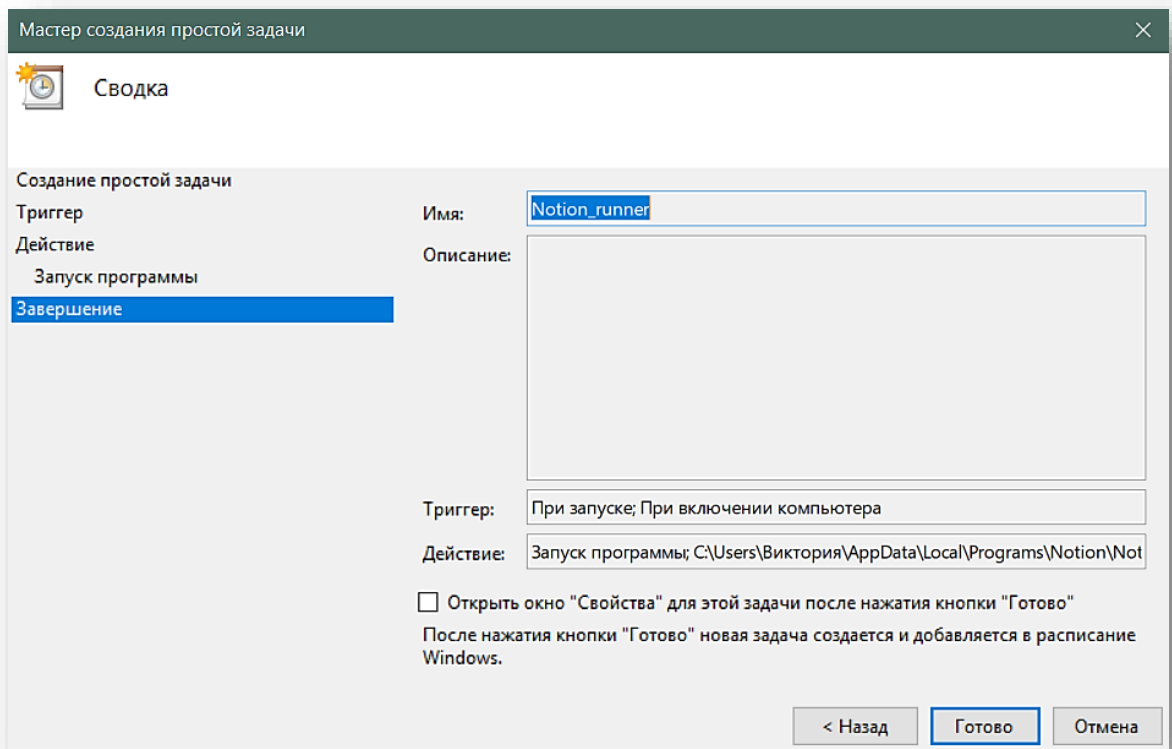
Повернути все як було ми можемо змінивши шлях в папці СтартАп на його попередній стан:



Далі використаємо Планувальник Задач для автоматичного запуску необхідних програм.

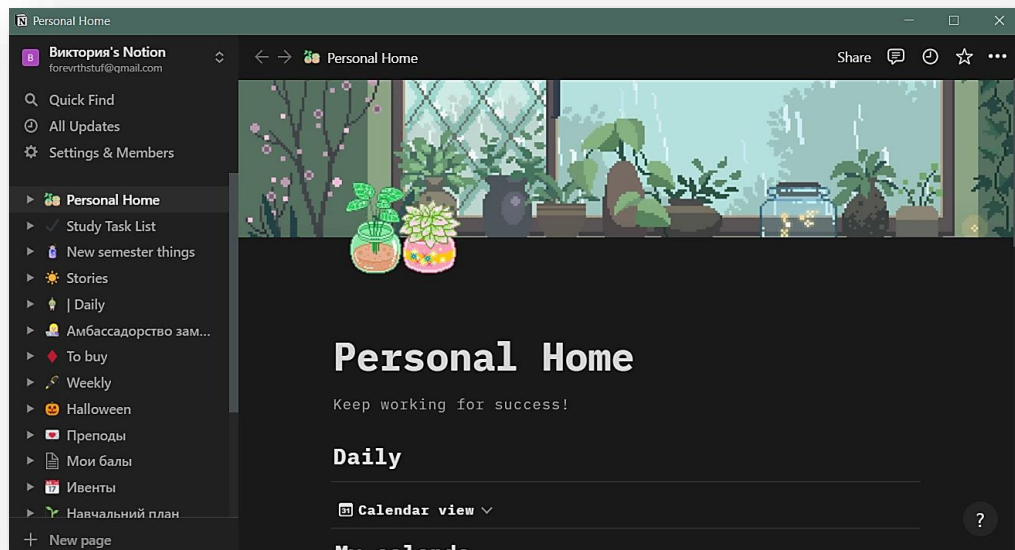


Щоб створити нову задачу, натискаємо «Создать простую задачу». Після цього у нас відкриється вікно, у якому ми проводимо налаштування нашої задачі:

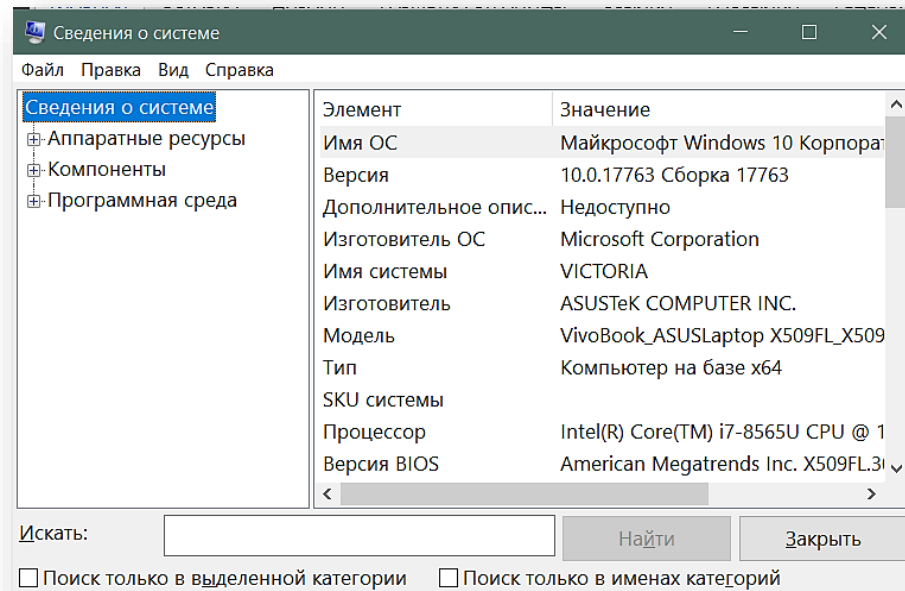


Натискаємо «Готово» та перезапускаємо комп'ютер.

Програма успішно запустилась:

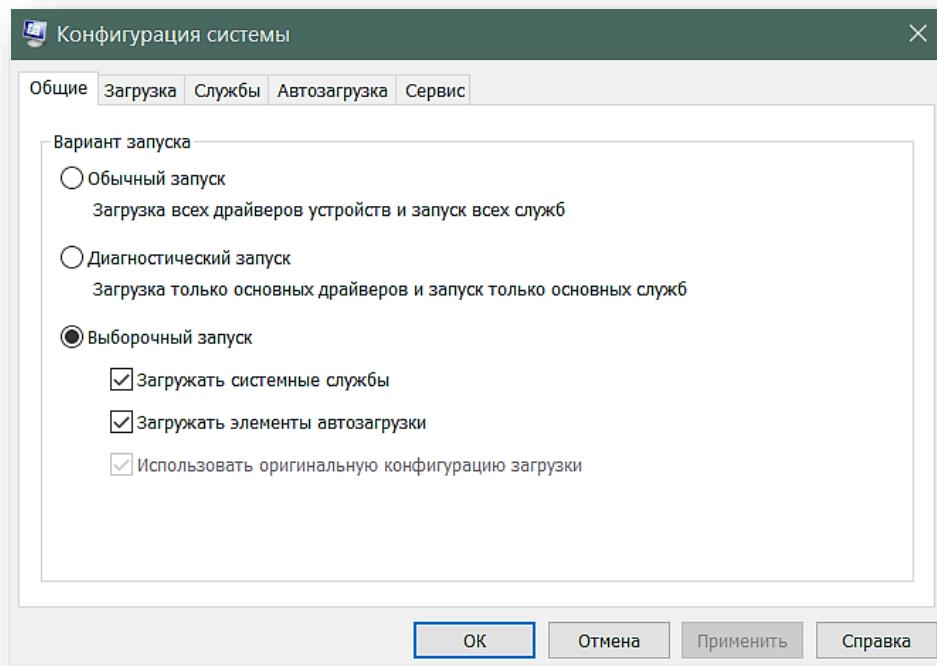


Далі перейдемо в програму «Відомості про систему». Це можна зробити у вікні Виконати за допомогою команди «msinfo32.exe».

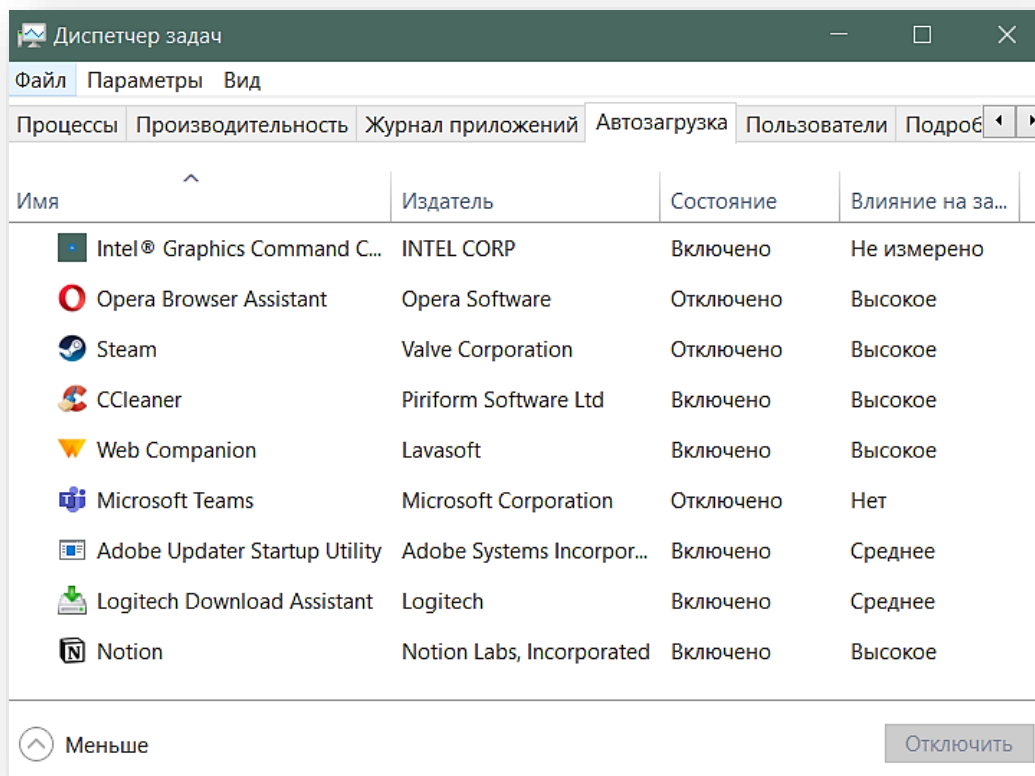


Нам потрібно перейти на вкладку «Программная среда» і обрати пункт «Автоматически запускаемые программы». Серед них якраз можемо побачити нашу програму, яку ми додали через планувальник завдань. Це свідчить про те, що наша операція успішно спрацювала і планувальник завдань – зручний і відмінно працюючий засіб для створення задач з автозавантаженням.

Також перевіримо список задач через утиліту «Конфігурація системи» (для цього нам потрібна команда «msconfig»)



Переходимо на вкладку «Автозагрузка» і натискаємо «Диспетчер задач»:

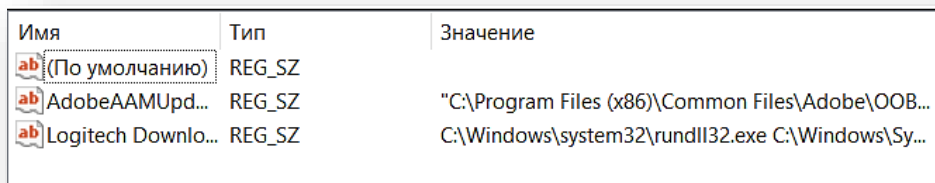


Як бачимо список програм співпадає зі списками в системному реєстрі та відомостях у системі.

Тепер я відключу автозавантаження для програми, яку я додала, бо я не завжди її використовую відразу після завантаження комп'ютера.

Щоб відключити задачу, потрібно обрати дану програму та натиснути «відключити». Після перезапуску комп'ютера програма не відкрилась, отже, ми зі своєю задачею впорались.

Далі перевіримо формування підрозділів для тимчасово виключених з автозавантаження програм ( "Run-") і наявність параметрів в цих підрозділі: HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	
AdobeAAMUpd...	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OOB...
Logitech Downlo...	REG_SZ	C:\Windows\system32\rundll32.exe C:\Windows\Sy...

Після перевірки не було знайдено жодного параметра. Значить ніяких програм у нас на автозапуск не стоїть.

Також для управління автозапуском можна використовувати сторонні програми, наприклад Starter, StartUp extractor, Ainvo startup manager, Autoruns.

## **Висновок:**

Для того, щоб попрацювати з автозапуском програм на комп'ютері, ми спробували такі способи:

► Переходимо назад до реєстру. Нам потрібно переглянути усі гілки, що відповідають за автозавантаження та зафіксувати їх вміст скріншотами.

Спочатку перевіряємо вміст гілки:

- Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

- Компьютер\HKEY\_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion

- Компьютер\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion

Тепер переглянемо папки автозавантаження та зафіксуємо їх вміст скріншотами. Для цього використаємо Провідник:

Переглянувши вміст цих папок, можемо побачити що вони пусті. Це свідчить про те, що ні одна програма не запускається автоматично при увімкненні комп'ютера.

Тепер створимо свою папку для автозавантаження та додамо до неї ярлик програми, яку ми хочемо завантажувати одразу після ввімкнення пристрою:

Для зміни папки автозавантаження в реєстрі потрібно перейти шляхом:

HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ User Shell Folders.

Тепер обираємо «StartUp» та замінюємо у ньому шлях до нашої створеної папки.

Після перезавантаження комп'ютера запустилась програма, яку я додала до папки автозавантажень:

Повернути все як було ми можемо змінивши шлях в папці СтартАп на його попередній стан:

Далі використаємо Планувальник Задач для автоматичного запуску необхідних програм.

Щоб створити нову задачу, натискаємо «Создать простую задачу». Після цього у нас відкриється вікно, у якому ми проводимо налаштування нашої задачі:

Натискаємо «Готово» та перезапускаємо комп'ютер.

Програма успішно запустилась:

Далі перейдемо в програму «Відомості про систему». Це можна зробити у вікні Виконати за допомогою команди «msinfo32.exe».

Нам потрібно перейти на вкладку «Программная среда» і обрати пункт «Автоматически запускаемые программы». Серед них якраз можемо побачити нашу програму, яку ми додали через планувальник завдань. Це свідчить про те, що наша операція успішно спрацювала і планувальник завдань – зручний і відмінно працюючий засіб для створення задач з автозавантаженням.

Також перевіримо список задач через утиліту «Конфігурація системи» (для цього нам потрібна команда «msconfig»)

Переходимо на вкладку «Автозагрузка» і натискаємо «Диспетчер задач»:



Як бачимо список програм співпадає зі списками в системному реєстрі та відомостях у системі.

Тепер я відключу автозавантаження для програми, яку я додала, бо я не завжди її використовую відразу після завантаження комп'ютера.

Щоб відключити задачу, потрібно обрати дану програму та натиснути «відключити». Після перезапуску комп'ютера програма не відкрилась, отже, ми зі своєю задачею впорались.

Далі перевіримо формування підрозділів для тимчасово виключених з автозавантаження програм ( "Run-") і наявність параметрів в цих підрозділі: HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run. Після перевірки не було знайдено жодного параметра.

Значить ніяких програм у нас на автозапуск не стоїть.

### **Контрольні питання:**

**1. Навіщо потрібно контролювати процес автозавантаження в операційній системі?**

Це необхідно для того, щоб з'ясувати, які програми завантажуються не під наглядом користувача таким чином можна виявити завантаження вірусних програм, а також оптимізувати свою роботу за комп'ютером.

**2. Перелічіть основні способи додавання програми в папку автозавантаження.**

Завантаження за допомогою файлів ініціалізації, завантаження за допомогою програми «Планувальник завдань», папки «Автозавантаження» в диспетчері завдань.

### **3. Для чого потрібен «Планувальник завдань»?**

Планувальник допомагає користувачу автоматизувати задачі, які він виконує щоразу під час роботи з системою. Також за допомогою планувальника можна налагодити процеси, які будуть виконуватись не потребуючи «ручної» взаємодії користувача.

### **4. Яким чином можна змінити папку автозавантаження?**

За допомогою зміни шляху папки автозавантаження у редакторі реєстру, а точніше за шляхом HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ User Shell Folders "Startup"=»c:\mystartup"

### **5. Яку роль відіграє редактор реєстру для програм автозавантаження?**

За допомогою редактору реєстрів можна налаштовувати автозавантаження, при цьому ці програми не будуть відображатись в папці «Автозавантаження»

### **6. Перелічіть основні підрозділи розділу автозавантаження редактору реєстру?**

Усередині цих розділів можуть розміщуватися такі підрозділи:

- \Run
- \RunOnce
- \RunOnce\Setup
- \RunOnceEx

- \RunServices
- \RunServicesOnce

Крім того, можуть бути присутніми підрозділи, які мають такі ж назви, до

яких додано знак "-", наприклад:

- \Run-
- \RunServices-

і т.д.

## **7. В якому порядку відбувається завантаження програм в ОС WINDOWS?**

У тих операційних системах, в яких підтримуються всі розділи,

перегляд підрозділів виконується в наступному порядку:

1. HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
 \ CurrentVersion \

RunServicesOnce

2. HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
 \ CurrentVersion \

RunServices

3. <Запит на вхід і реєстрацію користувача в операційній системі>

4. HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
 \ CurrentVersion \

RunOnce

5. HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
 \ CurrentVersion \

Run

6. HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \ CurrentVersion \

Run

7. Папка «Автозавантаження»

8. HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \ CurrentVersion \

RunOnce

За виключенням підрозділу HKEY\_LOCAL\_MACHINE\...\RunOnce, всі підрозділи і записи в них завантажуються асинхронно, тобто не чекаючи закінчення запуску всіх програм з підрозділів, які проглядається операційною системою раніше. Таким чином, наприклад, всі програми, перераховані в підрозділах "RunServices" і "RunServicesOnce" можуть виконуватися одночасно,

причому їх запуск може тривати і після входу користувача в ОС Windows.

Параметри розділу HKEY\_LOCAL\_MACHINE\...\RunOnce завантажуються синхронно. Це означає, що його записи не почнуть завантажуватися, поки не закінчиться завантаження розділів "RunServicesOnce" і "RunServices" і не завершиться автентифікація користувача. Тільки після того, як буде завершено завантаження всіх програм, зазначених в його параметрах, почнуть завантажуватися параметри розділів HKEY\_LOCAL\_MACHINE\...\Run,

HKEY\_CURRENT\_USER\...\Run,  
HKEY\_CURRENT\_USER\...\RunOnce і папки  
"Автозавантаження"

## **8. Яким чином можна налаштувати заборону на автозавантаження**

Крім видалення окремих параметрів з розділів, описаних вище, є способи відразу заборонити обробку параметрів, включених в певні розділи і стосуються певних режимів завантаження.

### 1. Не обробляти список для старих версій

Блокується автозапуск програм з наступних розділів реєстру:

HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
\CurrentVersion\Run

І HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \  
CurrentVersion \ Run

Для цього в розділі HKEY\_LOCAL\_MACHINE \ Software \  
Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer створюється  
наступний параметр DWORD зі значенням  
1:"DisableLocalMachineRun"=dword:00000001,

А в розділі HKEY\_CURRENT\_USER \ Software \ Microsoft \  
Windows \ CurrentVersion \ Policies \ Explorer параметр  
"DisableLocalUserRun"=dword:00000001.

### 2. Блокування автозавантаження програм виконуваних один раз

Аналогічно діє заборона списку Run Once для розділів  
HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Windows  
\CurrentVersion \ RunOnce і HKEY\_CURRENT\_USER \ Software \

Microsoft \ Windows \ CurrentVersion \ RunOnce. Для цього в згаданих в пункті 1 розділах реєстру створюються, відповідно, параметри: "DisableLocalMachineRunOnce"=dword:00000001 і "DisableLocalUserRunOnce"=dword:00000001, кожен з яких керує автозавантаженням в своєму розділі реєстру. Аналогічного ефекту можна також домогтися за допомогою налаштувань групової політики: "Конфігурація комп'ютеру – Адміністративні шаблони – Система – Не обробляти список автозапуску" для старих версій, а також "Конфігурація системи – Загальні – Вибірковий запуск – прибрати галочку із Завантаження елементів автозавантаження" для нових версій.