Практична робота № 4.

Налаштовування автоматичного запуску додатків та сервісів при завантаженні ОС Windows за допомогою Autoruns

Мета роботи — одержання практичних навичок роботи з утилітою Autoruns, консоллю Перегляд подій, редактором реєстру regedit для налаштовування автоматичного запуску додатків та сервісів при завантаженні ОС Windows.

- Робота виконується на основній або віртуальній машині із ОС Windows.
- Використовується програма Autoruns, системні утиліти: Редактор реєстру (regedit.exe), консоль Перегляд подій (eventvwr.exe).

Теоретичні відомості

Завантаження ОС Windows та автоматичний запуск додатків

Завантаження операційної Windows системи є складним процесом і складається із декількох етапів. Розглянемо його на прикладі BIOS, MBR для ОС Windows 7.

1. Виконання коду BIOS та MBR (UEFI,GPT) для тестування обладнання, визначення пристрою завантаження, визначення активного розділу, запуск менеджера завантаження Windows.

2. Менеджер завантаження (файл bootmgr.exe) зчитує дані конфігурації системи, які зберігаються у файлі BCD (Boot Configuration Data). При наявності декількох записів у файлі BCD буде відображено меню вибору операційної системи. Файл BCD знаходиться у папці Boot активного розділу.

3. Після вибору системи запускаються модуль завантаження операційної системи Winload.exe, компоненти ядра Ntoskrnl.exe і Hal.dll, системні служби і інші компоненти — цей етап супроводжується виведенням анімованого екрану з логотипом Windows.

4. Завантажується процес winlogon.exe, який керує входом користувачів в систему. Якщо на комп'ютері є всього один обліковий запис, не захищений паролем, вхід буде виконаний автоматично. В іншому випадку система буде очікувати вибору імені користувача і введення пароля.

5. У процесі входу в систему запускаються елементи автозавантаження, які прописані в реєстрі Windows і папці Автозавантаження.

Завантаження ОС Windows триває до повного завантаження робочого столу, тобто до припинення активності процесів, що беруть участь у завантаженні.

Для налаштування автоматичного запуску (автозавантаження) додатків, фонових сервісів і скриптів при завантаженні ОС Windows (крок 5), як правило, використовуються:

- розділи реєстру Run;
- папка «Автозавантаження»;
- сервіси операційної системи;
- завдання планувальника і скрипти групової політики, що виконуються при вході користувача в систему.

Програми з перших трьох пунктів цього списку можна побачити в утиліті msconfig.exe. Зауважимо, що, починаючи з Windows 8.1, частина функцій msconfig.exe для швидкого управління програмами в автозавантаженні винесено в Диспетчер завдань.

Для гнучкого налаштування запуску сервісів системи можна скористатися консоллю services.msc.

Для керування завданнями планувальника та скриптами групової політики призначені консолі taskschd.msc та **gpedit.msc** відповідно.

Найбільш повну картину автозавантаження дає утиліта Autoruns.

Можливості утиліти Autoruns

Для того, щоб дізнатися про всі процеси, які були запущені разом з вашою системою, вам допоможе утиліта Autoruns від Sysinternals, останню версію якої можна знайти за адресою https://technet.microsoft.com/uk-ua/sysinternals.

Програма Autoruns від Марка Русиновича і Брайса Когсуелла допомагає перевіряти максимальну кількість розміщень автозапуску на наявність програм, налаштованих на запуск в процесі завантаження або входу в систему, на відміну від будь-яких інших програм моніторингу автозапуску. Ця програма абсолютно безкоштовна і до однієї з її переваг можна віднести те, що всі програми відображаються у тому порядку, в якому операційна система обробляє їх. Із даною

програмою можна працювати як під 32-розрядними, так і під 64-розрядними операційними системами Windows.

Детальний опис можливостей та інтерфейсу програми наведено в рекомендаціях до виконання практичної роботи №4, які розміщено у методичних вказівках «Операційна система Windows. Частина 3», що доступні за адресою http://fpm.kpi.ua/archive/dir.do.

Налаштування запуску програм автоматично при старті ОС

Налаштувати запуск програм автоматично при старті ОС можна декількома способами [1].

1. Запуск додатків при вході користувача в систему

Якщо програма може бути запущена при вході користувача в систему, вона відобразиться на вкладці «Logon» в Autoruns. При цьому є наступні варіанти розміщення програми в автозапуску:

1.1. Запис про її автозапуск прописаний у реєстрі:

- HKCU\Software\Microsoft\ CurrentVersion\Run;
- HKCU\Software\Microsoft\CurrentVersion\RunOnce;
- HKLM\Software\Microsoft\CurrentVersion\Run;
- HKLM\Software\Microsoft\Windows\CurrentVersion\ RunOnce.

Додатково (цих розділів може не бути у вас в реєстрі), подивіться наступні місця:

- HKLM Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run;
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\ RunOnce;
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run;
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run.

У відповідній гілці реєстру Windows створюється запис про програму, що завантажується. В якості назви він має назву програми, в якості значення — запис шляху до виконуваного файлу з опціями.

При «вимкненні» програми із автозавантаження через Autoruns у відповідній гілці Autoruns створює папку AutorunsDisabled, куди переміщує запис про відповідну програму. Таким чином, при потребі можливе швидке відновлення програми у автозапуску.

Якщо виконати «видалення» відповідного запису, то він назавжди видалиться із реєстру.

Для налаштування автозавантаження додатків у ОС Windows традиційно використовується утиліта Конфігурація системи (msconfig.exe). Починаючи з Windows 8.1 частина функцій msconfig.exe для швидкого управління програмами в автозавантаженні винесено в Диспетчер завдань (рис. 1).

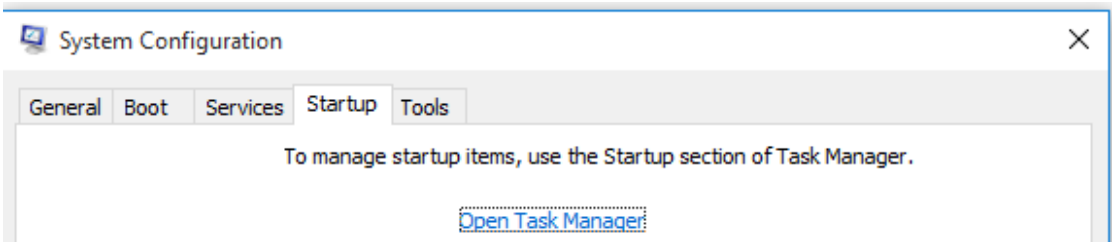

Рис. 1а. Вкладка Автозавантаження утиліти msconfig

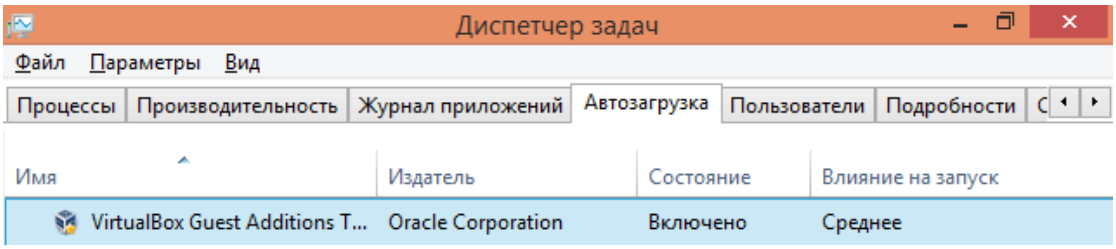

Рис. 1б. Вкладка Автозавантаження Диспетчера завдань Windows 8.1

1.2. Для автозапуску програми при завантаженні ОС в одній із папок Startup в файловій системі можна розмістити її ярлик:

- «%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup»;
- «C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup» (щоб потрапити в цю папку, можна ввести у вікно «Виконати» системне посилання на папку автозавантаження shell:startup).

При «вимкненні» програми із автозавантаження через Autoruns програма створює у відповідній гілці папку AutorunsDisabled, куди переміщує запис про відповідну програму. Таким чином, при потребі можливе швидке відновлення програми у автозапуску.

Якщо виконати «видалення» відповідного запису, то він назавжди видалиться із Startup.

2. Запуск додатків через Планувальник завдань

Крім додатків, що запускаються автоматично з операційною системою, ви можете переглянути всі завдання, що призначені на запуск Планувальником завдань.

Якщо включити записи Microsoft і Windows, то виявиться, що в системі заплановано дуже багато завдань. Лише частина із них має відношення до процесу завантаження ОС.

Завдання, для яких вказані тригери «При запуску» та «При вході в систему», стосуються процесу завантаження ОС і будуть виконані при настанні відповідної події.

3.Налаштування запуску сервісів та драйверів

Записи про сервісні процеси (системні та окремих програм) та драйвери можна відредагувати на вкладках **Services та Drivers** програми Autoruns відповідно.

Записи про сервіси також можна відредагувати безпосередньо в реєстрі за адресою: HKLM\SYSTEM\CurrentControlSet\services\.

Для кожного сервісу є параметр «Start» типу «REG_DWORD». Він може приймати таке значення:

0 — Низькорівневі драйвери, наприклад, драйвери дисків, які завантажуються на самому ранньому етапі завантаження — завантаження ядра;

1 — Драйвери, які завантажуються після ініціалізації ядра ОС;

2 — Драйвери та послуги, які повинні бути завантажені диспетчером управління службами (дорівнює параметру — «Авто») ;

3 — Драйвери та служби, що запускаються диспетчером управління службами тільки в разі отримання явної інструкції на завантаження (дорівнює параметру — «Вручну»);

4 — Драйвери та служби, які не завантажуються (дорівнює параметру — «Відключено»).

Якщо для сервісу вказати параметр запуску «Автоматичний (відкладений запуск)», то запуск сервісу відбудеться не відразу. При цьому значення параметру Start у реєстрі буде «0x02», але з’явиться новий параметр, який вказує саме на затримку запуску (DelayedAutostart=”0x01”).

При «вимкненні» сервісу із автозавантаження через Autoruns у відповідному розділі створюється параметр AutorunsDisabled, значення якого зберігає рівень, з яким раніше запускався сервіс. Таким чином, при потребі, можливе швидке відновлення автозапуску сервісу з відповідним рівнем запуску.

Якщо виконати «видалення» відповідного запису через Autoruns, то він назавжди видалиться із реєстру.

Налаштування сервісів (служб) ОС Windows

Всі служби ОС Windows можна умовно розділити на три групи:

- служби, які не можна відключати;
- служби, які можна відключити практично на будь-якому комп'ютері, тому що в більшості випадків вони не потрібні;
- служби, які можна відключити на домашньому комп'ютері або ноутбуці (без мережі).

Консоль Перегляд подій

У системі Windows для перегляду системних журналів використовується консоль **Перегляд подій** (Event Viewer — eventvwr.exe). «Перегляд подій» входить до складу консолі Управління комп'ютером (Computer Management).

З його допомогою можна переглядати Журнал системи (System), що містить записи про події, які реєструються системними компонентами Windows. Журнал зберігає події операційної системи або її компонентів, наприклад, невдачі при запусках служб або ініціалізації драйверів, загальносистемні повідомлення та інші повідомлення, що відносяться до системи в цілому. За замовчуванням він розміщується в %SystemRoot%\System32\Winevt\Logs\System.Evtx

У журналах реєструються 5 типів подій:

Помилка (Error) — подія реєструється у випадку виникнення серйозної події (такої, як втрата даних або функціональних можливостей). Подія даного типу буде зареєстрована, якщо неможливо завантажити який-небудь сервіс у ході запуску системи.

Попередження (Warning) — подія не серйозна, але може привести до виникнення проблем у майбутньому. Наприклад, якщо недостатньо дискового простору, то в журнал буде занесене попередження.

Повідомлення (Information) — значима подія, яка свідчить про успішне завершення операції прикладною програмою, драйвером або сервісом. Така подія може, наприклад, зареєструвати мережний драйвер, що успішно завантажився.

Аудит успіхів (Success Audit) — подія, відповідна успішно завершеній дії, пов'язаній із підтримкою безпеки системи. Прикладом такої події є успішна спроба входу користувача в систему.

Аудит відмов (Failure Audit) — подія, відповідна невдало завершеній дії, пов'язаній із підтримкою безпеки системи. Наприклад, така подія буде зареєстрована, якщо спроба доступу користувачем до мережного диска закінчилася невдачею.

Маніпуляції із автозавантаженням додатків та сервісів впливають на час завантаження системи. Для оцінки тривалості завантаження ОС використовується Журнал додатків та служб Microsoft (Просмотр событий — Журнал приложений и служб Microsoft — Windows — Diagnostics — Performance — журнал «Работает»). Запис про подію із кодом 100 (100 — це pid процесу завантаження ОС) дає змогу оцінити швидкість завантаження ОС.

Завдання на практичну роботу

1. В ОС своєї віртуальної машини зробити копію реєстру (гілок HKEY_LOCAL_MACHINE\SOFTWARE\, HKEY_LOCAL_MACHINE\SYSTEM\).
2. За допомогою консолі Перегляд подій (eventvwr.exe) визначити час завантаження ОС. Розмістити отримане значення у звіт (таблиця 1).
3. За допомогою утиліти Autoruns (запуск від імені адміністратора) налаштувати додатки, які не є системними (приховати записи Windows):

3.1. налаштувати додатки, які запускаються при старті ОС (Logon):

3.1.1. створити запис автозавантаження для Autoruns від імені адміністратора через папку Автозавантаження;

3.1.2. встановити CCleaner http://www.piriform.com/ccleaner та створити запис автозавантаження для CCleaner через реєстр (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run);

3.1.3. встановити Skype та відключити його автозавантаження через Autoruns.

https://www.skype.com/en/download-skype/skype-for-windows/downloading/

При встановленні програми вона прописується на автозавантаження у реєстр. Потрібно відключити її автозавантаження через Autoruns;

3.1.4. за потреби відключити із автозавантаження інші програми;

3.1.5. перезавантажити систему. Визначити час завантаження системи і записати його у таблицю 1.

3.2. дослідити і налаштувати сервіси, які є сервісами додатків (не ОС) (Services):

3.2.1. для SkypeUpdate через реєстр встановити запуск сервісу вручну (параметр Start=3); зробити експорт відповідної гілки реєстру в файл SkypeUpdate.reg;

3.2.2. за потреби відключити із автозавантаження інші сервіси;

3.3. на вкладці Драйвери видалити драйвери, які відображаються жовтим кольором;

3.4. перезавантажити систему. Визначити час завантаження системи і записати його у таблицю 1.

4. Провести налаштування запуску сервісів ОС Windows через Autoruns:

4.1. відповідно до варіанта налаштувати на автоматичний запуск сервіс із таблиці 2;

4.2. відповідно до варіанта налаштувати на запуск вручну сервіс із таблиці 3;

4.3. відповідно до варіанта відключити сервіс із таблиці 4.

Якщо відповідний сервіс відсутній, оберіть довільний із відповідної таблиці.

4.4. Виконати експорт гілок реєстру, які відповідають завданням 4.1-4.3.

4.5. Перезавантажити систему. Визначити час завантаження системи і записати його у таблицю 1.

5. За допомогою консолі Перегляд подій (eventvwr.exe) проаналізувати:

5.1. як змінився час завантаження системи;

5.2. чи виникли в системі події (критичні, помилки, попередження), пов’язані із налаштуваннями сервісів (Просмотр событий — Журналы Windows — Система). Зробити знімок екрану. Якщо так, то виправити відповідні налаштування.

6. При увімкнених записах Windows та Microsoft зберегти через Autoruns записи про налаштування автозапуску у файл №варіанту.txt.

7. Доповнити файл №варіанта.txt записами із файлів п.4.4 (reg-файлів).

8. Заповнити таблицю 1 та оформити звіт.

Таблиця 1. Результати автоналаштувань додатків та сервісів

Версія ОС	
Час завантаження системи	до правок _____ після змін: 1 (програми) _____ 2 (сервіси програм та драйвери)_____ 3 (сервіси ОС) _____
Додатки, які запускаються при старті ОС	додано через папку: додано через реєстр: вимкнено через Autoruns:
Сервіси додатків	змінено через запис реєстру:
Сервіси ОС	
автоматичний запуск	
запуск вручну	
відключено сервіс	
Помилки, попередження (консоль Перегляд подій)	
відсутні/наявні	

Підготовка до виконання практичної роботи

Ознайомтеся з рекомендаціями до виконання практичної роботи №4, які розміщено у методичних вказівках «Операційна система Windows. Частина 3», що доступні за адресою http://fpm.kpi.ua/archive/dir.do.

Вимоги до оформлення результатів роботи

1. Електронний звіт про практичну роботу повинен мати назву N.doc, де N – номер студента за списком, і містити:

1) титульний аркуш;
2) заповнену таблицю 1; 1 рисунок;
3) висновки з виконання практичної роботи.

До захисту друкуються пункти 1, 2 електронного звіту.

2. Файл результату N.txt (utf-8, Windows) має складатися із 4 структурних елементів, які відокремлені порожніми рядками:

1) завдання 6;
2) завдання 7.

3. На Системі Moodle електронного порталу коледжу викладаються файли N.txt, N.doc.
4. Неохідно продемонструвати файли експорту реєстру.

Питання для самоперевірки

1. Процес завантаження ОС Windows.
2. Рівні завантаження сервісів та драйверів.
3. Які тригери в Планувальнику завдань пов’язані із завантаженням ОС?
4. Як у реєстрі відображається запис про програми із вкладки Logon при їх включенні та відключенні.
5. Що таке запуск програми "вручну"?
6. Чим запуск програми «автоматично» відрізняється від запуску «автоматично відкладено». Яким значенням у реєстрі відповідають ці рівні запуску.
7. Які можна дати рекомендації щодо включення та відключення автозавантаження програм та сервісів?
8. Можливості та інтерфейс програми Autoruns.
9. Призначення сервісів ОС Windows (відповідно до номеру варіанта).

Рекомендована література

1. http://www.outsidethebox.ms/12581/
2. http://www.outsidethebox.ms/11296/