

## ПАРКТИЧНЕ ЗАНЯТТЯ 3

### ІНСТРУМЕНТАЛЬНІ ЗАСОБИ WINDOWS ДЛЯ ВІДСТЕЖУВАННЯ СИСТЕМНИХ ПРОЦЕСІВ

#### 3.1 Мета заняття

Познайомитися з окремими інструментальними засобами ОС Windows та основними прийомами роботи з командним рядком на прикладі системних процесів та процесів, які працюють у режимі користувача.

#### 3.2 Теоретичні положення

Одним з унікальних атрибутів, які стосуються процесу і не відображаються більшістю інструментальних засобів, є ідентифікатор батьківського процесу або процесу-творця (parent or creator process ID). Це значення можна отримати за допомогою Системного монітора (Performance Monitor) або програмним засобом, шляхом запиту Creating Process ID. Дерево процесів може показати такий засіб, як tree.

Щоб переглянути список процесів, які виконуються у поточний момент на локальному або віддаленому комп'ютері з вікна командного рядка, можна скористатися інструментальним засобом tasklist.exe.

Команда tasklist /svc дозволить переглянути список процесів та служб для кожного процесу.

Таблиця 3.1 – Фрагмент переліку процесів і служб.

Ім'я образу	PID	Служби
System Idle Process	0	Н/Д
System	4	Н/Д
smss.exe	520	Н/Д
csrss.exe	588	Н/Д
wininit.exe	636	Н/Д
csrss.exe	648	Н/Д
services.exe	684	Н/Д
lsass.exe	696	KeyIso, SamSs
lsm.exe	704	Н/Д
winlogon.exe	808	Н/Д
svchost.exe	896	DcomLaunch, PlugPlay
svchost.exe	956	RpcSs
svchost.exe	1064	Audiosrv, Dhcp, Eventlog, lmhosts
svchost.exe	1088	AudioEndpointBuilder, EMDMgmt, hidserv, Netman, PcaSvc, SysMain, TabletInputService, TrkWks, UxSms, WdiSystemHost, Wlansvc, WPDBusEnum, wudfsvc
.....		
.....		
unsecapp.exe	2824	Н/Д

WmiPrvSE.exe	2956	Н/Д
WINWORD.EXE	1892	Н/Д
cmd.exe	3348	Н/Д
conime.exe	3352	Н/Д
tasklist.exe	3308	Н/Д

### Взаємодія процесів

Щоб показати взаємодію кожного процесу з його батьківськими і дочірніми процесами, застосовують відступи. Процеси, батьки яких припинили своє існування, вирівняні по лівому краю, оскільки, навіть за наявності прабатьківського процесу, способів виявлення зв'язку з ними просто не існує. Windows зберігає тільки ідентифікатор процесу-творця і не дає посилань на творця цього творця і так далі.

Щоб продемонструвати той факт, що Windows не відслідковує більше одного ідентифікатора батьківського процесу, виконайте наступні дії:

1. Відкрийте вікно командного рядка.
2. Наберіть title Parent, щоб змінити заголовок вікна на «Parent» (батьківський).
3. Наберіть start cmd (що призведе до запуску другого вікна командного рядка).
4. Наберіть у другому вікні командного рядка title Child, щоб змінити заголовок вікна на «Child» (дочірній).
5. Відкрийте Диспетчер завдань.
6. Наберіть у другому вікні командного рядка notepad (команду, яка запускає Microsoft Notepad).
7. Знову зверніться до другого вікна командного рядка і наберіть exit. (Зауважте, що Notepad залишається в робочому стані.)
8. Перейдіть до Диспетчера завдань.
9. Натисніть на вкладку Details. Знайдіть Notepad.exe, перегляньте властивості. Завешіть дерево процесів cmd (через контекстне меню).

Вікна командного рядка зникнуть, але вікно програми Notepad залишиться відкритим, оскільки воно було нащадком у другому поколінні завершеного процесу командного рядка. Оскільки проміжний процес (батьківський по відношенню до Notepad) був завершений, зв'язок між батьківським процесом і його нащадком у другому поколінні був втрачений.

### Порівняння часу роботи у режимі ядра і у режимі користувача

Щоб подивитися, скільки часу ваша система працює в режимі ядра порівняно з роботою у призначеному для користувача режимі, можна скористатися Системним монітором (Performance Monitor). Виконайте наступні дії:

1. Запустіть Системний монітор (Performance Monitor): "Win+R" і ввести perfmon. На розташованому зліва деревовидному списку інструментів Продуктивність (Performance) оберіть пункти Засоби спостереження (Monitoring Tools) → Системний монітор (Performance Monitor).

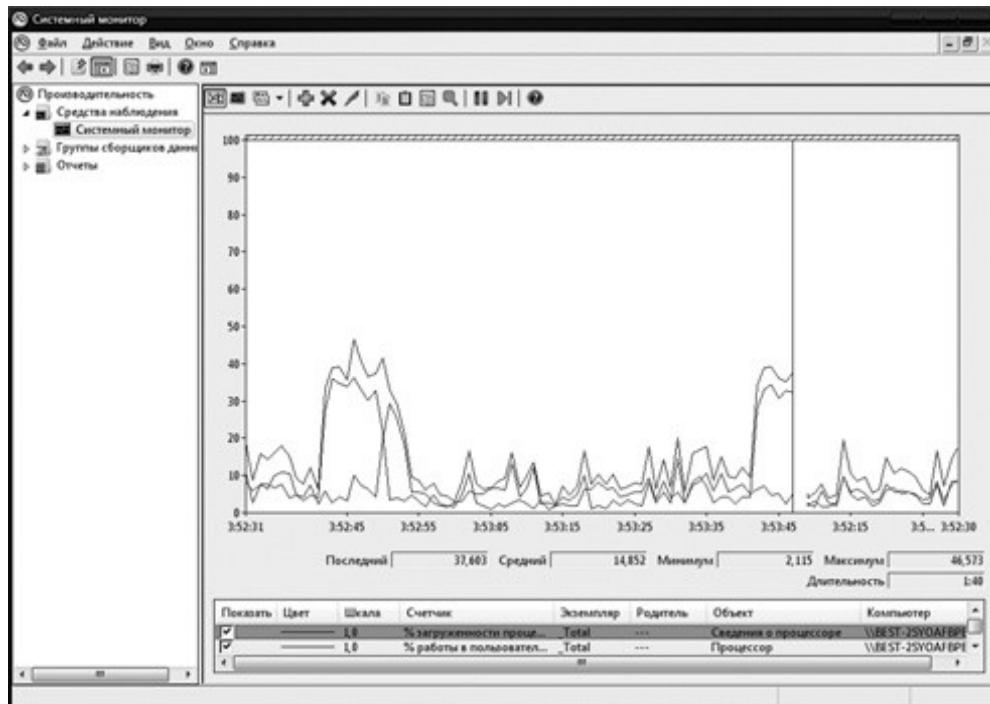


Рисунок 3.2 – Системный монітор

2. Натисніть на кнопку додавання (+), яка знаходиться на панелі інструментів.

3. Розкрийте розділ лічильників Процесор (Processor), натисніть на пункті роботи у привілейованому режимі (% Privileged Time counter) і, утримуючи в натиснутому стані клавішу Ctrl, натисніть на пункті роботи у режимі користувача (% User Time).

4. Натисніть на кнопку Додати (Add), а потім на кнопку ОК.

5. Відкрийте вікно командного рядка і проведіть безпосереднє сканування свого диска C по мережі, набравши команду:

dir \\%computername%\c\$/s.

6. Після закінчення роботи закрийте вікно інструментального засобу.

Щоб побачити, скільки часу в режимі ядра і в призначеному для користувача режимі використовує сам Системний монітор (Performance Monitor), запустіть його ще раз, але при цьому додайте окремі лічильники процесу роботи у режимі користувача (% User Time) і роботи у привілейованому режимі (% Privileged Time) для кожного процесу в системі:

1. Якщо Системний монітор (Performance Monitor) не запущений, запустіть його знову. (Якщо він вже запущений, почніть роботу з порожнього відображення, натиснувши в області графіків правою кнопкою миші і обравши пункт Видалити всі лічильники (Remove All Counters).)

2. Натисніть на кнопці додавання (+), яка знаходиться на панелі інструментів.

3. У доступній області лічильників розкрийте розділ Процес (Process).

4. Оберіть лічильники роботи в режимі користувача (% User Time) і роботи в привілейованому режимі (% Privileged Time).

5. Оберіть кілька процесів в області Примірники обраного об'єкта (Instance) (наприклад, mmc, csrss і Idle).

6. Натисніть на кнопку Додати (Add), а потім на кнопку ОК.

7. Інтенсивно порухайте мишею у різні боки.

8. Оберіть на панелі інструментів пункт Виділити (Highlight) або натисніть клавіші Ctrl + H, щоб включити режим виділення. Поточний обраний лічильник буде виділено чорним кольором.

9. Прокрутіть список лічильників вниз для визначення процесів, чії потоки були запущені при переміщенні покажчика миші, і зверніть увагу на те, в якому режимі вони були запущені, у призначеному для користувача або у режимі ядра.

Таким чином можна побачити (знайшовши в стовпці Примірник (Instance) процес mmc), що графік часу виконання процесу, який належить Системному моніторові, в режимі ядра і в призначеному для користувача режимі при переміщенні миші пішов вгору, оскільки в ньому виконується прикладної код в призначеному для користувача режимі, і викликаються Windows-функції, які запускаються в режимі ядра. Зверніть також увагу на активність потоку, який належить процесові csrss і виконується в режимі ядра при переміщенні миші.

Ця активність виникає завдяки тому, що цьому процесові належить вихідний потік введення тієї підсистеми Windows, що виконується в режимі ядра, яка обробляє введення з клавіатури і миші. І нарешті, процес Idle, який, як можна помітити, витрачає майже 100% свого часу на роботу в режимі ядра, насправді процесом не є, це псевдопроцес, який використовують для підрахунку порожніх циклів центрального процесора.

Судячи з режиму, в якому запускаються потоки процесу Idle, коли Windows нічого не робить, процес очікування відбувається в режимі ядра.

#### Перегляд встановлених драйверів пристроїв

Отримати перелік встановлених драйверів можна шляхом запуску msinfo32 ("Win+R" і ввести msinfo32). У розділі Відомості про систему (System Summary) розкрийте пункт Програмне середовище (Software Environment) і відкрийте вікно Системні драйвери (System Drivers).

#### Перегляд інформації про процеси за допомогою Диспетчера завдань

Диспетчер завдань надає короткий список процесів, які виконуються у системі. Запустити його можна:

1) натиснувши клавіші Ctrl + Shift + Esc;

2) натиснувши правою кнопкою миші на панелі завдань з наступним вибором пункту Диспетчер завдань;

3) натиснувши клавіші Ctrl + Alt + Delete з подальшим вибором Диспетчера завдань;

4) натиснувши "Win+R" ввести Taskmgr.exe.

Щоб побачити перелік процесів, потрібно після запуску Диспетчера завдань натиснути на вкладку Процеси. Зверніть увагу на те, що процеси ідентифікуються за іменами тих образів, екземплярами яких вони є. На відміну від деяких об'єктів Windows, процесам можна давати глобальні імена.

Task Manager

File Options View

Processes	Performance	App history	Startup	Users	Details	Services
Name	1% CPU	55% Memory	0% Disk	0% Network	0% GPU	GPU Engine
> Antimalware Service Executable	0%	176.4 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D
> Microsoft Word (2)	0%	67.4 MB	0 MB/s	0 Mbps	0%	
> Service Host: Local System (Net...	0%	55.3 MB	0 MB/s	0 Mbps	0%	
> Windows Shell Experience Host ...	0%	31.4 MB	0 MB/s	0 Mbps	0%	
> Task Manager	0.5%	26.2 MB	0 MB/s	0 Mbps	0%	
Windows Explorer	0%	23.5 MB	0 MB/s	0 Mbps	0%	
WMI Provider Host	0%	23.4 MB	0 MB/s	0 Mbps	0%	
> Service Host: Local Service (No ...	0%	23.0 MB	0 MB/s	0 Mbps	0%	
> Cortana (2)	0%	18.9 MB	0 MB/s	0 Mbps	0%	
Desktop Window Manager	0.2%	16.8 MB	0 MB/s	0 Mbps	0.1%	
> Service Host: DCOM Server Pro...	0.4%	14.9 MB	0 MB/s	0 Mbps	0%	GPU 0 - Copy
> Microsoft Windows Search Inde...	0%	13.0 MB	0 MB/s	0 Mbps	0%	

Рисунок 3.1 – Фрагмент переліку процесів.

Щоб подивитися додаткову інформацію про процеси, оберіть у меню "Вид" пункт "Показати стовпці" і відзначте ті стовпці, які потрібно додати.

Диспетчер завдань містить наступні вкладки:

1. Процеси (Processes): список запущених додатків і фонових процесів у системі разом з інформацією про процесор, пам'яті, диск, мережу, графічний процесор та інші ресурси.

2. Продуктивність (Performance): графіки в реальному часі, що показують загальне використання ресурсів ЦП, пам'яті, диску, мережі та графічного процесора системи.

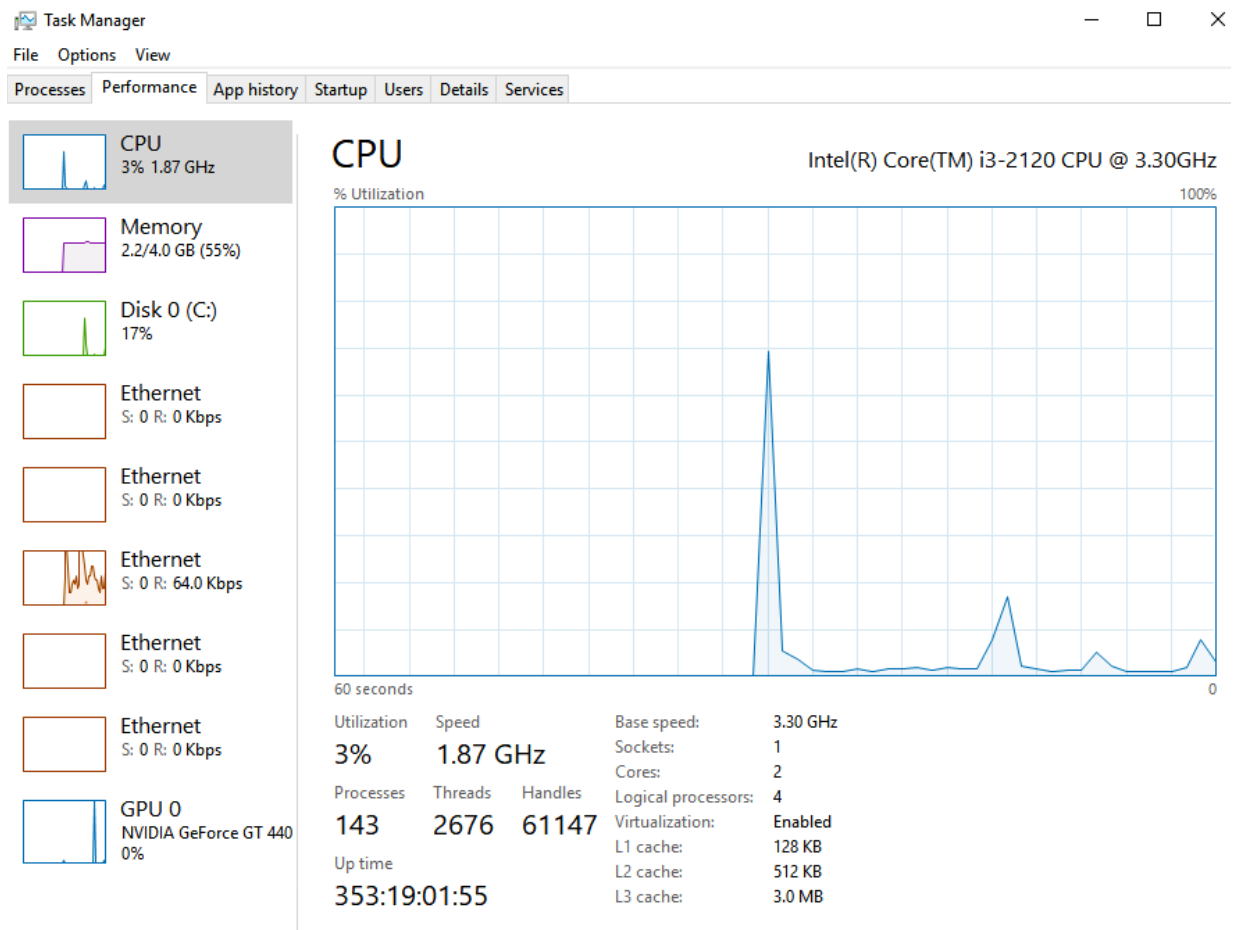


Рисунок 3.2 – Фрагмент вкладки "Продуктивність"

Тут можна переглянути подробиці: IP-адресу комп'ютера, назву моделі процесора, графічного процесора та ін.

3. Історія додатків (App history): інформація про те, скільки ресурсів ЦП і додатків мережі використано для поточного облікового запису користувача.

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Resource usage since 1/16/2021 for current user account.  
[Delete usage history](#)

Name	CPU time	Network	Metered network	Tile updates
3D Builder	0:00:00	0 MB	0 MB	0 MB
3D Viewer	0:00:00	0 MB	0 MB	0 MB
Alarms & Clock	0:00:00	0 MB	0 MB	0 MB
Calculator	0:00:00	0 MB	0 MB	0 MB
Camera	0:00:00	0 MB	0 MB	0 MB
Connect	0:00:00	0 MB	0 MB	0 MB
Cortana	0:00:13	1.0 MB	0 MB	0 MB
Feedback Hub	0:00:01	0 MB	0 MB	0 MB
Get Help	0:00:00	0 MB	0 MB	0 MB
Groove Music	0:00:00	0 MB	0 MB	0 MB
> Mail and Calendar (2)	0:00:01	0 MB	0 MB	0 MB
Maps	0:00:00	0 MB	0 MB	0 MB
Messaging	0:00:00	0 MB	0 MB	0 MB
Microsoft Edge	0:00:00	0 MB	0 MB	0 MB
> Microsoft Photos (2)	0:00:00	0 MB	0 MB	0 MB
Microsoft Solitaire Collec...	0:00:00	0 MB	0 MB	0 MB
Microsoft Store	0:00:01	0 MB	0 MB	0 MB
Mixed Reality Portal	0:00:00	0 MB	0 MB	0 MB

Рисунок 3.3 – Фрагмент історії додатків

Це стосується тільки нових додатків універсальної платформи Windows (UWP), іншими словами, до додатків Store, а не до традиційних додатків Windows для настільних ПК (додатки Win32).

4. Автозавантаження (Startup): список програм, які автоматично запускаються при вході в обліковий запис користувача.

Task Manager

File Options View

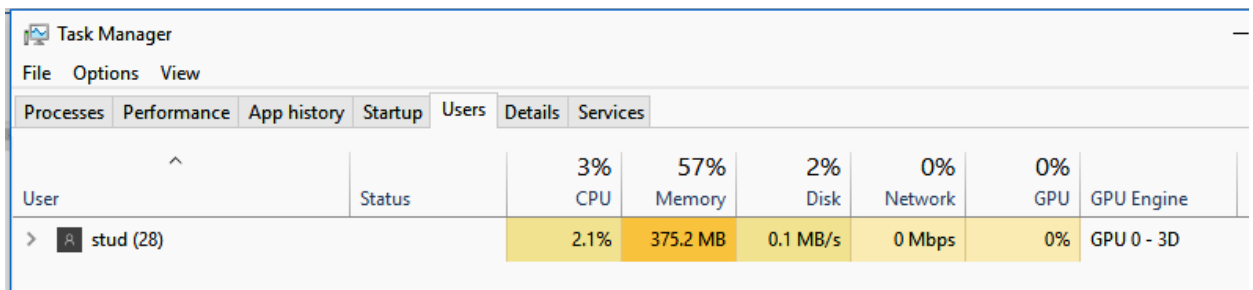
Processes Performance App history Startup Users Details Services

Name	Publisher	Status	Startup impact
Java Update Scheduler	Oracle Corporation	Enabled	Low
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Virus		Enabled	Not measured
VMware Tray Process	VMware, Inc.	Enabled	Low
Windows Defender notificati...	Microsoft Corporation	Enabled	Low

Рисунок 3.4 – Фрагмент автозавантаження

Можна вимкнути автозавантаження програм з Диспетчера завдань (це також можна зробити з Налаштування> Програми> Автомат).

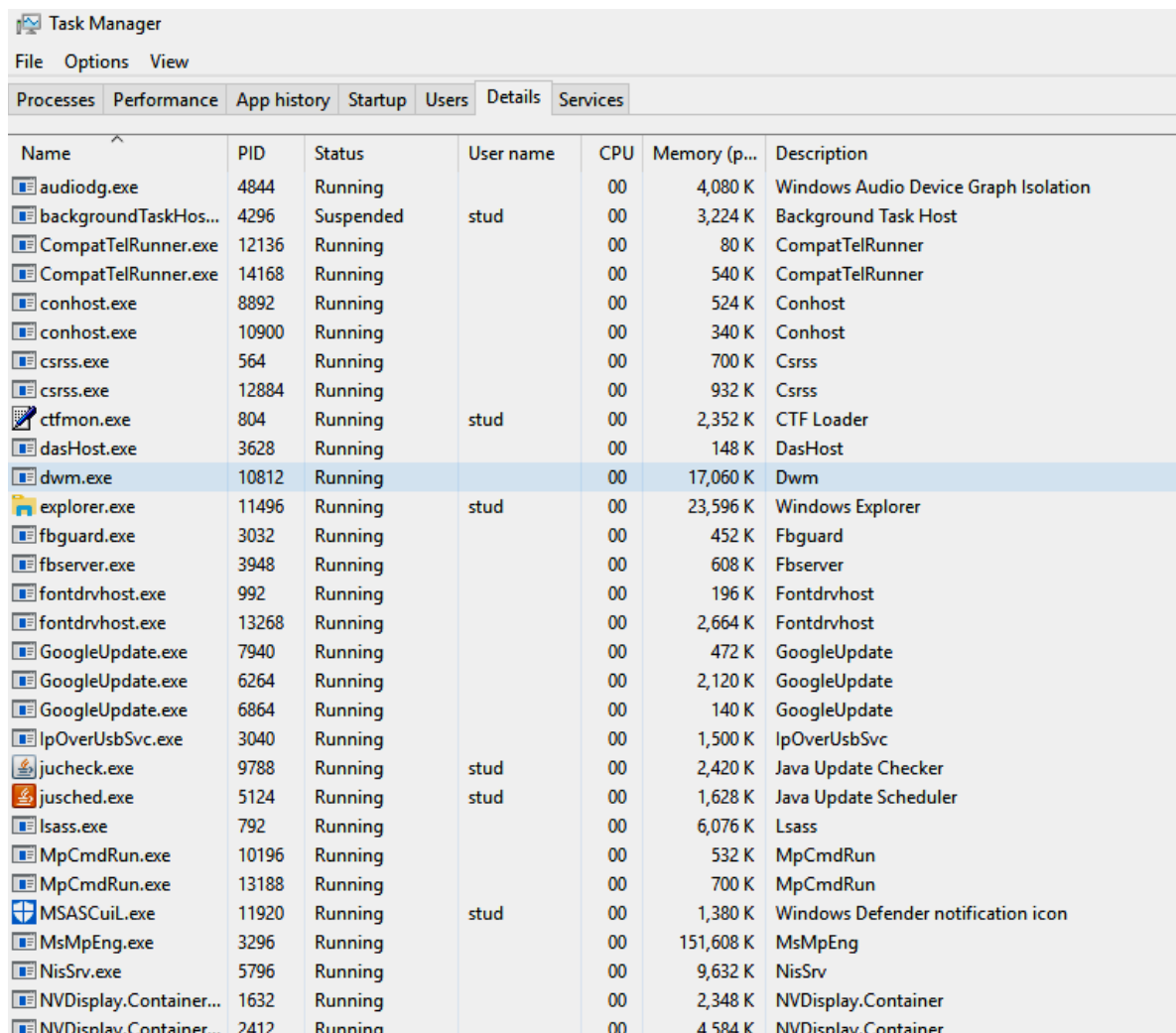
5. Користувачі (Users): обліковий запис користувача, які в даний момент зайшов на ПК, скільки ресурсів і які програми він використовує.



User	Status	CPU	Memory	Disk	Network	GPU	GPU Engine
stud (28)		2.1%	375.2 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D

Рисунок 3.5 – Фрагмент вкладки "Користувачі"

6. Детально (Details): більш детальна інформація про процеси, запущені у системі.

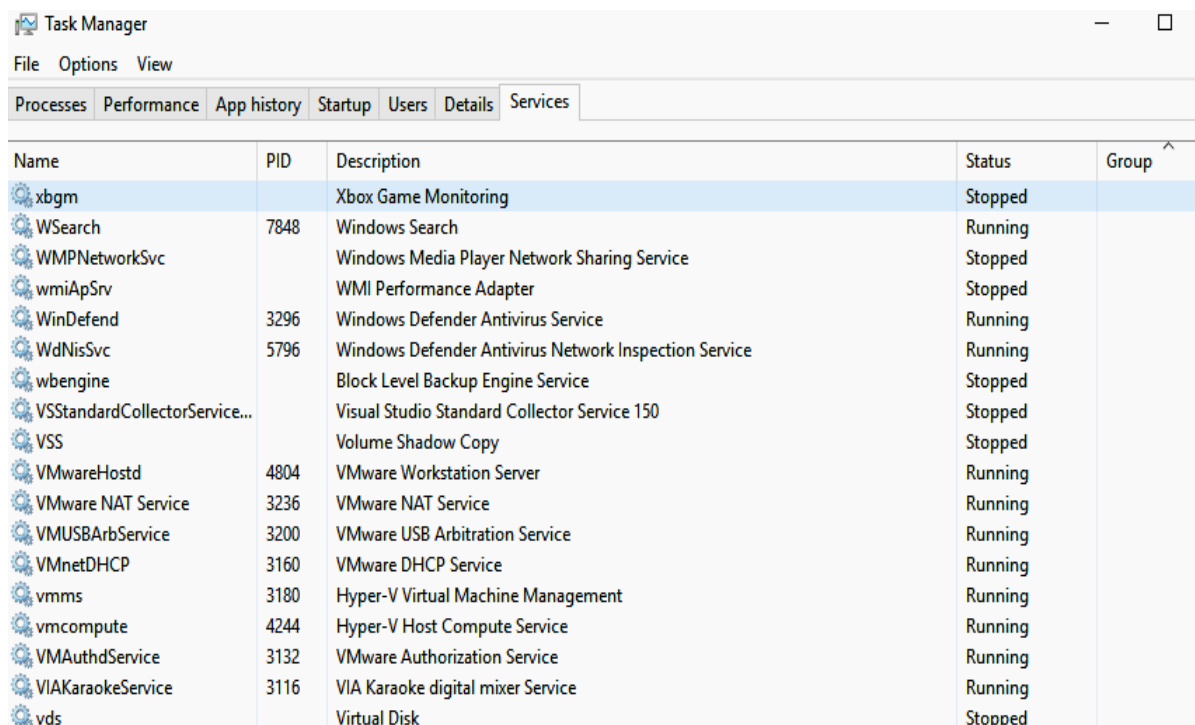


Name	PID	Status	User name	CPU	Memory (p...	Description
audiodg.exe	4844	Running		00	4,080 K	Windows Audio Device Graph Isolation
backgroundTaskHos...	4296	Suspended	stud	00	3,224 K	Background Task Host
CompatTelRunner.exe	12136	Running		00	80 K	CompatTelRunner
CompatTelRunner.exe	14168	Running		00	540 K	CompatTelRunner
conhost.exe	8892	Running		00	524 K	Conhost
conhost.exe	10900	Running		00	340 K	Conhost
csrss.exe	564	Running		00	700 K	Csrss
csrss.exe	12884	Running		00	932 K	Csrss
ctfmon.exe	804	Running	stud	00	2,352 K	CTF Loader
dasHost.exe	3628	Running		00	148 K	DasHost
dwm.exe	10812	Running		00	17,060 K	Dwm
explorer.exe	11496	Running	stud	00	23,596 K	Windows Explorer
fbguard.exe	3032	Running		00	452 K	Fbguard
fbserver.exe	3948	Running		00	608 K	Fbserver
fontdrvhost.exe	992	Running		00	196 K	Fontdrvhost
fontdrvhost.exe	13268	Running		00	2,664 K	Fontdrvhost
GoogleUpdate.exe	7940	Running		00	472 K	GoogleUpdate
GoogleUpdate.exe	6264	Running		00	2,120 K	GoogleUpdate
GoogleUpdate.exe	6864	Running		00	140 K	GoogleUpdate
IpOverUsbSvc.exe	3040	Running		00	1,500 K	IpOverUsbSvc
jucheck.exe	9788	Running	stud	00	2,420 K	Java Update Checker
jusched.exe	5124	Running	stud	00	1,628 K	Java Update Scheduler
lsass.exe	792	Running		00	6,076 K	Lsass
MpCmdRun.exe	10196	Running		00	532 K	MpCmdRun
MpCmdRun.exe	13188	Running		00	700 K	MpCmdRun
MSASCuiL.exe	11920	Running	stud	00	1,380 K	Windows Defender notification icon
MsMpEng.exe	3296	Running		00	151,608 K	MsMpEng
NisSrv.exe	5796	Running		00	9,632 K	NisSrv
NVDisplay.Container...	1632	Running		00	2,348 K	NVDisplay.Container
NVDisplav.Container...	2412	Running		00	4,584 K	NVDisplav.Container

Рисунок 3.5 – Фрагмент вкладки "Детально"



7. Сервіси (Services): Управління системними сервісами (цю інформацію можна отримати через services.msc, консоль управління службами).



Name	PID	Description	Status	Group ^
xboxgm		Xbox Game Monitoring	Stopped	
WSearch	7848	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sharing Service	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3296	Windows Defender Antivirus Service	Running	
WdNisSvc	5796	Windows Defender Antivirus Network Inspection Service	Running	
wbengine		Block Level Backup Engine Service	Stopped	
VSSStandardCollectorService...		Visual Studio Standard Collector Service 150	Stopped	
VSS		Volume Shadow Copy	Stopped	
VMwareHostd	4804	VMware Workstation Server	Running	
VMware NAT Service	3236	VMware NAT Service	Running	
VMUSBArbService	3200	VMware USB Arbitration Service	Running	
VMnetDHCP	3160	VMware DHCP Service	Running	
vmms	3180	Hyper-V Virtual Machine Management	Running	
vmcompute	4244	Hyper-V Host Compute Service	Running	
VMAuthdService	3132	VMware Authorization Service	Running	
VIAKaraokeService	3116	VIA Karaoke digital mixer Service	Running	
vds		Virtual Disk	Stopped	

Рисунок 3.5 – Фрагмент вкладки "Сервіси"

За допомогою правої кнопки миші можна:

1. Перемикається на: перемикання у вікно потрібної програми, виведення його на передню частину робочого столу і фокусування на ньому.
2. Завершити завдання: завершити процес.
3. Запуск нового завдання: відкриється вікно «Створити нову задачу», де можна вказати адресу програми, папки, документа або веб-сайту, і Windows відкриє його.
4. Завжди зверху: зробіть вікно Диспетчера завдань поверх інших вікон на робочому столі.
5. Відкрити розташування файлу: відкрити вікно провідника, що показує розташування файлу .exe програми.
6. Пошук в Інтернеті: пошук Bing за ім'ям додатку/ім'ям файлу програми.
7. Властивості: відкрийте вікно властивостей для файлу .exe програми. Тут ви можете налаштувати параметри сумісності і подивитися, наприклад, номер версії програми.

#### Управління процесами

На вкладці «Процеси» список процесів можна відсортувати за іменами, він буде розбитий на три категорії. Група «Додатки» показує список запущених додатків. Дві інші категорії – це фонові та системні процеси. Наприклад, такі інструменти, як Dropbox, антивірусна програма, процеси

фонового оновлення і апаратні утиліти зі значками області повідомлень (на панелі завдань) відображаються у списку фонових процесів.

Дії, які можна виконувати над процесами за допомогою контекстного меню:

1. Розгорнути: Деякі додатки, такі як Google Chrome, мають кілька процесів (кожна вкладка одного вікна буде новим процесом). Інші додатки мають кілька вікон, які є частиною одного процесу.

2. Згорнути: Згорнути розширену групу.

3. Завершити завдання: завершити процес.

4. Перезавантаження: цей параметр з'являється тільки при натисканні правою кнопкою миші у провіднику Windows. Це дозволяє перезапустити explorer.exe замість простого завершення завдання. У старіших версіях Windows необхідно було завершити завдання Explorer.exe, а потім запустити його вручну, щоб усунути проблеми з робочим столом Windows, панеллю задач або меню «Пуск».

5. Значення ресурсу: дозволяє обрати відсоткові або точні значення у мегабайтах для пам'яті, диска та мережі.

6. Створити файл дампу: це інструмент налаштування для програмістів. Він захоплює знімок пам'яті програми і зберігає його на диск.

7. Перейти до деталей: перейдіть до процесу на вкладці "Детально", щоб побачити більш детальну технічну інформацію.

8. Розташування файлу: відкриває провідник з обраним файлом .exe.

9. Пошук в Інтернеті: пошук за назвою процесу на Bing.

10. Властивості: відкриває вікно властивостей файлу .exe, пов'язаного з процесом.

На цій вкладці також відображається детальна інформація про кожний процес і спільне використання ресурсів. Можна натиснути правою кнопкою миші на заголовки у верхній частині списку та обрати потрібні стовпчики. Значення у кожному стовпчику мають колірне кодування, а темніший помаранчевий (або червоний) колір вказує на більш широке використання ресурсів. Вміст стовпчика можна сортувати, наприклад, обрати стовпчик ЦП, щоб побачити запущені процеси, відсортовані за використання ЦП з найбільшим завантаженням ЦП. У верхній частині стовпчика також показано загальне використання ресурсів усіма процесами системи. Можна перетягувати стовпчики, щоб змінити їх порядок. У наявності є такі стовпчики:

Тип: категорія процесу, яка є додатком, фоновим або системним процесом.

Статус: якщо програма зависла, тут відображається повідомлення «Не відповідає». Програми іноді починають відповідати через деякий час, а іноді залишаються завислими. Якщо Windows призупинила програму для економії енергії, у цьому стовпчику з'явиться зелений лист. Сучасні програми UWP можуть призупиняти енергозбереження, а Windows також може припиняти роботу традиційних настільних додатків.

Видавець: ім'я видавця програми. Наприклад, Chrome відображає «Google Inc.», а Microsoft Word відображає «Microsoft Corporation».

PID: ідентифікатор процесу, який Windows пов'язала з процесом. Ідентифікатор процесу може використовуватися окремими функціями або системними утилітами. Windows призначає унікальний ідентифікатор процесові під час кожного запуску програми. Ідентифікатор процесу дозволяє розрізняти кілька запущених процесів, якщо запущено кілька екземплярів однієї і тієї ж програми.

Ім'я процесу: ім'я файлу процесу. Наприклад, File Explorer – це файл explorer.exe, Microsoft Word – це WINWORD.EXE, а сам Диспетчер завдань – Taskmgr.exe.

Командний рядок: повний командний рядок, що використовується для запуску процесу. Тут показаний повний шлях до файлу .exe процесу (наприклад, «C:\WINDOWS\Explorer.exe»), а також усі параметри командного рядка, використані для запуску програми.

ЦП: завантаження ЦП процесу, що відображається у відсотках від загального обсягу доступних ресурсів ЦП.

Пам'ять: обсяг фізичної робочої пам'яті системи, яку використовує процес у даний момент, відображається у МБ/ГБ.

Диск: активність диска, створювана процесом, відображається як МБ/с. Якщо процес не читає або не записує на диск у даний момент, він буде відображати 0 МБ/с.

Мережа: використання мережі процесом у поточній первинній мережі, що відображається у Мбіт/с.

Графічний процесор: ресурси графічного процесора, що використовуються процесом, відображаються у відсотках від доступних ресурсів графічного процесора.

Механізм графічного процесора: пристрій і процесор графічного процесора, що використовуються процесом. Якщо у системі декілька графічних процесорів, це покаже, який саме графічний процесор використовує процес. (вкладка «Детально», щоб дізнатися, який номер («GPU 0» або «GPU 1» пов'язаний з яким фізичним GPU).

Енергоспоживання: передбачуване енергоспоживання процесу з урахуванням поточної активності процесора, диска і графічного процесора.

Тенденція енергоспоживання: передбачуваний вплив на енергоспоживання з плином часу. Столпчик Power Usage просто показує поточне енергоспоживання, але цей столпчик відстежує енергоспоживання з плином часу. Наприклад, якщо програма час від часу споживає багато енергії, але загальне споживання не високе, у столпчику енергоспоживання може бути написано «Дуже низьке», а у столпчику «Тенденція енергоспоживання» – «Висока» або «Помірна».

Перегляд інформації про продуктивність

На вкладці «Продуктивність» відображаються графіки у реальному часі, що відображають використання системних ресурсів, таких як процесор,

пам'ять, диск, мережа і графічний процесор. Якщо є кілька дисків, мережевих пристроїв або графічних процесорів, ви відображаються окремо. Графік показує використання ресурсів за останні 60 секунд. На додаток до інформації про ресурси на сторінці «Продуктивність» відображається інформація про обладнання системи, наприклад:

**Процесор:** назва і номер моделі процесора, його швидкість, кількість ядер, а також включені і доступні функції віртуалізації обладнання. Він також показує «час безвідмовної роботи» системи, тобто скільки часу система працює з моменту останнього завантаження.

**Пам'ять:** скільки оперативної пам'яті, її швидкість і скільки слотів оперативної пам'яті на материнській платі, скільки пам'яті у даний час заповнено кешованими даними. ОС Windows вважає це «резервом». Ці дані будуть готові і "чекають", поки це буде потрібно системі, але ОС автоматично скине кешовані дані і звільнить місце, якщо це буде потрібно більше пам'яті для іншої задачі.

**Диск:** назва і номер моделі диску, його розмір і поточна швидкість читання і запису.

**Wi-Fi або Ethernet:** Windows відображає тут ім'я мережевого адаптера і його IP-адреси (як IPv4, так і IPv6). Для підключень Wi-Fi можна побачити стандарт Wi-Fi, який використовується у поточному підключенні, наприклад, 802.11ac.

**Графічний процесор:** на панелі графічного процесора показані окремі графіки для різних видів діяльності – наприклад, 3D або відео кодування або декодування. Графічний процесор має власну вбудовану пам'ять, тому показане використання пам'яті графічним процесором, назва і номер моделі графічного процесора, версія графічного драйвера.

Можна контролювати використання графічного процесора прямо з Диспетчера завдань без будь-якого стороннього програмного забезпечення. Кнопка «Відкрити монітор ресурсів» у нижній частині вікна відкриває інструмент «Монітор ресурсів», який надає більш детальну інформацію про використання графічного процесора, пам'яті, диска та мережі окремими запущеними процесами.

### Історія додатків

Вкладка «Історія додатків» застосовується тільки до додатків універсальної платформи Windows (UWP). Вона не відображає інформацію про традиційні настільні додатки Windows. У верхній частині вікна відображено дату, коли Windows почала збирати дані про використання ресурсів. У списку відображаються додатки UWP, а також кількість процесорного часу і мережевої активності, які додаток згенерував з цієї дати.

**Наявні опції:**

**CPU Time:** кількість процесорного часу, який програма використала протягом цього періоду.

**Мережа:** загальний обсяг даних, переданих програмою мережею за цей період.

Дозована мережа: обсяг даних, переданих по дозованим мережам. Можна налаштувати мережу як виміряну для збереження даних на ній. Ця опція призначена для мереж, в яких у користувача обмежені дані, наприклад, для мобільної мережі, до якої він прив'язується.

Оновлення листків: обсяг даних, завантажених програмою для відображення оновлених плиток у меню «Пуск» Windows 10.

Завантаження: кількість даних, завантажених програмою у всіх мережах.

#### Контроль запуску додатків

Вкладка «Автозавантаження» – це вбудований в Windows 10 диспетчер запуску програм. У ньому перераховані всі додатки, які Windows автоматично запускає для поточного облікового запису користувача. Наприклад, тут відображаються програми в папці «Автозавантаження» і програми, налаштовані для запуску у реєстрі Windows. Щоб вимкнути програму запуску, натисніть на неї правою кнопкою миші та оберіть "Вимкнути" або «Ввімкнути», щоб увімкнути.

У окремих версіях ОС Windows 10 у верхньому правому куті вікна можна побачити «Час останнього BIOS». Це показує, скільки часу знадобилося BIOS (або прошивці UEFI) для ініціалізації обладнання при останньому завантаженні ОС. Наявні опції:

Назва: назва програми.

Видавець: ім'я видавця програми.

Статус: тут відображається «Ввімкнено», якщо програма автоматично запускається при вході у систему або «Вимкнено», якщо завдання запуску вимкнене.

Вплив під час запуску: оцінка обсягу ресурсів процесора і диска, які програма використовує під час запуску. Windows вимірює і відстежує це у фоновому режимі. Полегшена програма покаже «Низький», а важка програма – «Високий», вимкнена програма – «Ні». Можна прискорити процес завантаження, вимкнувши програми з «високим» ефектом запуску.

Тип запуску: показує, чи запускається програма через запис у реєстрі («Registry») або через те, що вона знаходиться в папці автозавантаження («Folder.»).

Дискове введення-виведення під час запуску: дискова активність, яку програма виконує під час запуску, у МБ. Windows вимірює і записує це кожне завантаження.

CPU під час запуску: кількість процесорного часу, яку програма використовує під час запуску, у мс. Windows вимірює і записує це під час завантаження.

Виконується зараз: тут відображається слово «Виконується», якщо у даний момент програма запущена.

Disabled Time: для запуску програм, які вимкнули, тут відображається дата і час, коли вимкнули програму.

Командний рядок: показує повну командний рядок, з якого запускається програма, включаючи всі параметри командного рядка.

#### Перевірка користувачів

На вкладці «Користувачі» відображається список зареєстрованих користувачів, які виконали вхід (у тому числі тих, що заблокували свої облікові записи. Ці сеанси відображаються як "Вимкнено"), і їх запущених процесів.

Можна вимкнути обліковий запис користувача (контекстне меню - команда «Вимкнути», або «Вихід із системи»). Параметр «Вимкнути» перериває підключення до робочого столу, але програми продовжують працювати, і користувач може увійти назад, як у випадку блокування сеансу робочого столу. Параметр «Вихід із системи» завершує всі процеси, наприклад, вихід з Windows.

З цієї вкладки також можна керувати процесами облікового запису іншого користувача. Наявні опції:

Ідентифікатор: у кожного зареєстрованого облікового запису користувача є свій номер ідентифікатора сеансу. Сеанс «0» зарезервований для системних служб, інші програми можуть створювати свої власні облікові записи користувачів. Зазвичай не потрібно знати цей номер, тому він за замовчуванням прихований.

Сеанс: тип сеансу. Наприклад, «Консоль», якщо звернення відбувається у локальній системі (підходить для серверних систем з віддаленими робочими столами).

Ім'я клієнта: ім'я віддаленої клієнтської системи, що звертається до сеансу, якщо до нього звертаються віддалено.

Стан: стан сеансу. Наприклад, якщо сеанс користувача заблоковано, у статусі буде вказано «Вимкнено».

CPU: загальний процесор, який використовується процесами користувача.

Пам'ять: спільна пам'ять, яка використовується процесами користувача.

Диск: загальна активність диску, пов'язана з процесами користувача.

Мережа: загальна мережева активність від процесів користувача.

#### Детальні дані про процеси

Вкладка «Детально» надає додаткову інформацію та показує процеси з усіх облікових записів користувачів у системі. Додаткові параметри:

Завершити завдання: завершити процес.

Завершити дерево процесів: завершити процес і всі процеси, створені цим процесом.

Встановити пріоритет: встановити пріоритет для процесу: низький, нижче нормального, нормальний, вище нормального, високий і в реальному часі. Процеси запускаються з нормальним пріоритетом. Низький пріоритет ідеальний для фонових процесів, а більш високий – для процесів робочого столу.

**Встановити подібність:** встановити схожість процесорів з процесами, іншими словами, на якому процесорі виконується процес. За замовчуванням процеси виконуються на всіх процесорах системи. Проте, інколи потрібно обмежити процес певним процесором, наприклад, для старих ігор та інших програм, які передбачають наявність одного процесора (для програм кожне ядро виглядає як окремий процесор).

**Аналіз ланцюжка очікування:** черга, у якій процеси і потоки очікують доступ до ресурсу, зайнятого іншим процесом (інструмент налагодження для діагностики зависань).

**Віртуалізація контролю облікових записів:** ввімкнення/вимкнення віртуалізації контролю облікових записів для процесу. Ця функція виправляє додатки, яким потрібен доступ адміністратора, шляхом віртуалізації їх доступу до системних файлів, перенаправлення їх доступу до файлів і реєстру в інші папки. Зазвичай використовується старими програмами. Опція налаштування для розробників.

**Створити файл дампа:** зробити знімок пам'яті програми і зберегти його на диск. Це корисний інструмент налагодження для програмістів. **Розташування файлу:** відкрийте вікно провідника, що показує виконуваний файл процесу.

**Пошук в Інтернеті:** пошук Bing за назвою процесу.

**Властивості:** перегляд вікна властивостей .exe-файлу процесу.

**Перейти до сервісу (iv):** показати сервіси, пов'язані з процесом, на вкладці Сервіси.

**Стовпчики, які можна вивести у заголовок:**

**Ім'я пакета:** для додатків універсальної платформи Windows (UWP) відображається ім'я пакета додатка, з якого відбувається процес. Для інших додатків цей стовпець порожній. Додатки UWP зазвичай поширюються через Microsoft Store.

**PID:** унікальний ідентифікаційний номер процесу. Це пов'язано з процесом, а не з програмою – наприклад, якщо ви закриєте і знову відкриєте програму, новий процес отримає новий PID.

**Стан:** показує, чи запущений процес або припинений для економії енергії. Windows 10 завжди «призупиняє» додатки UWP, які не використовують для економії системних ресурсів (дозволяє контролювати, призупинення традиційних процесів на робочому столі).

**Ім'я користувача:** ім'я облікового запису користувача, на якому запущений процес (крім облікових записів користувачів будуть і системні, такі як SYSTEM і LOCAL SERVICE).

**Ідентифікатор сеансу:** унікальний номер, пов'язаний з сеансом користувача, на якому виконується процес.

**Ідентифікатор об'єкта завдання:** об'єкт завдання, в якому виконується процес. Об'єкти завдання – це спосіб угруповання процесів, щоб ними можна було керувати як групою.

**ЦП:** відсоток ресурсів ЦП, які використовує процес у даний час для всіх ЦП. Якщо ніщо інше не використовує процесорний час, Windows покаже

Системний процес простою. Іншими словами, якщо інші процеси системи використовують у сукупності 10%, ЦП простоює 90% часу.

Час ЦП: загальний час процесора (в секундах), використаний процесом з моменту його запуску. Якщо процес закривається і перезавантажується, він буде скинутий. Це хороший спосіб виявити процесори, завантажені процесом, які зараз можуть працювати вхолосту.

Цикл: відсоток циклів ЦП, який процес у даний час використовує для всіх ЦП.

Робочий набір (пам'ять): обсяг фізичної пам'яті, який використовується процесом у даний момент.

Піковий робочий набір (пам'ять): максимальний обсяг фізичної пам'яті, який використовується процесом.

Дельта робочого набору (пам'ять): зміна у пам'яті робочого набору з моменту останнього оновлення даних.

Пам'ять (активний приватний робочий набір): обсяг фізичної пам'яті, який використовується процесом, і який не може використовуватися іншими процесами. Процеси часто кешують деякі дані, щоб краще використовувати оперативну пам'ять, але можуть швидко звільнити цей простір пам'яті, якщо це знадобиться іншому процесові. Цей стовпчик виключає дані з призупинених процесів UWP.

Пам'ять (приватний робочий набір): обсяг фізичної пам'яті, який використовується процесом, який не може використовуватися іншими процесами. Цей стовпчик не виключає дані з призупинених процесів UWP.

Пам'ять (загальний робочий набір): обсяг фізичної пам'яті, яку використовує процес, який може використовуватися іншими процесами за необхідності.

Розмір фіксації: обсяг віртуальної пам'яті, яку Windows резервує для процесу.

Вивантажуваний пул: обсяг пам'яті ядра з можливістю підкачки, яку ядро Windows або драйвери виділяють для цього процесу. Операційна система може перемістити ці дані в файл підкачки за необхідності.

NP pool: обсяг не сторінкової пам'яті ядра, що виділяється ядром Windows або драйверами для цього процесу. Операційна система не може перемістити ці дані у файл підкачки.

Помилки сторінок: кількість помилок сторінок, згенерованих процесом з моменту його запуску. Це відбувається, коли програма намагається отримати доступ до пам'яті, яка для неї у даний момент не виділена.

PF Delta: зміна кількості збоїв сторінок з моменту останнього оновлення.

Базовий пріоритет: пріоритет процесу (низький, нормальний, високий). Системні фонові завдання, які не є терміновими, можуть мати низький пріоритет порівняно, наприклад, з процесами прикладних програм.

Дескриптори: поточна кількість дескрипторів у таблиці об'єктів процесу. Дескриптори представляють системні ресурси, такі як файли, ключі реєстру і потоки.



Threads: кількість активних потоків у процесі. Кожен процес запускає один або кілька потоків, і Windows виділяє їм час роботи процесора. Потоки ділять пам'ять пам'ять процесу.

Призначені для користувача об'єкти: кількість «віконних менеджерів», які використовуються процесом (вікна, меню і курсори).

Об'єкти GDI: кількість об'єктів інтерфейсу графічного пристрою, використаних процесом. Вони використовуються для відображення призначеного для користувача інтерфейсу.

Операції читання вводу-виводу: кількість операцій читання, виконаних процесом з моменту його запуску. Введення/виведення розшифровується як введення/виведення. Складається з файлу, мережі та пристрою вводу/виводу.

Операції введення/виведення: кількість операцій запису, виконаних процесом з моменту його запуску.

Інша введення/виведення: число операцій не читання і запису, виконаних процесом з моменту його запуску. Наприклад, функції управління.

Число прочитаних байтів вводу/виводу: загальна кількість байтів, прочитаних процесом з моменту його запуску.

Байт запису введення/виведення: загальна кількість байтів, записаних процесом з моменту його запуску.

Інші байти введення/виведення: загальне число байтів, використаних в операціях введення/виводу без читання і без запису з моменту запуску процесу.

Шлях до зображення: повний шлях до виконуваного файлу процесу.

Командний рядок: точний командний рядок, з якої був запущений процес, включаючи виконуваний файл і всі аргументи командного рядка.

Контекст операційної системи: мінімальна операційна система, з якою сумісна програма, якщо будь-яка інформація включена в файл маніфесту програми (наприклад, «Windows Vista», «Windows 7», «Windows 8.1»). Більшість взагалі нічого не відображає в цьому стовпці.

Платформа: 32-розрядний або 64-розрядний процес.

Підвищені: незалежно від того, чи запущений процес у режимі підвищених прав (іншими словами, з правами адміністратора) чи ні.

Віртуалізація контролю облікових записів: чи включена для процесу віртуалізація контролю облікових записів. Це віртуалізує доступ програми до реєстру і файлової системи, дозволяючи програмами, розробленими для більш старих версій Windows, працювати без доступу адміністратора. Опції можуть бути: «Ввімкнено», «Вимкнено» і «Не дозволено» – для процесів, яким потрібен доступ до системи.

Опис: зручний для читання опис процесу з файлу .exe. Наприклад, chrome.exe має опис «Google Chrome», а explorer.exe – «Провідник Windows».

Запобігання виконанню даних: функція безпеки, яка допомагає захистити додатки від атак (може бути ввімкнене/вимкнене).

Корпоративний контекст: у доменах це показує, в якому корпоративному контексті виконується додаток. Це може бути контекст корпоративного домена з доступом до корпоративних ресурсів, «особистий»

контекст без доступу до робочих ресурсів або «виключення» для системних процесів Windows.

Регулювання потужності: ввімкнути або вимкнути регулювання потужності для процесу. Windows автоматично обмежує певні програми, коли ними не користуються для економії заряду батареї.

GPU: відсоток ресурсів GPU, використаних процесом, або, точніше, найвище використання серед всіх ядер GPU.

Ядро графічного процесора: ядро графічного процесора, яке використовує процес, або, більш конкретно, ядро графічного процесора, яке процес використовує найчастіше. Наприклад, навіть якщо у вас тільки один графічний процесор, він, ймовірно, має різні механізми для 3D-візуалізації, кодування відео і декодування відео.

Виділена пам'ять графічного процесора: загальний обсяг пам'яті графічного процесора, який процес використовує у всіх графічних процесорах. Графічні процесори мають власну виділену відеопам'ять, вбудовану у дискретні графічні процесори, і зарезервовану частину звичайної системної пам'яті на вбудованих графічних процесорах.

Shared GPU memory: загальний обсяг системної пам'яті, використаної спільно з графічним процесором, який використовується процесом. Це відноситься до даних, що зберігаються у оперативній пам'яті, яка використовується спільно з графічним процесором, а не до даних, що зберігаються у виділеній вбудованій пам'яті графічного процесора.

### Робота з сервісами

На вкладці «Сервіси» відображається список системних служб ОС Windows. Це фонові завдання, які виконує Windows, навіть якщо обліковий запис користувача не зареєстрований. Ними керує ОС Windows. Залежно від сервісу, він може запускатися автоматично під час завантаження або тільки за необхідності.

Багато сервісів є частиною самої Windows 10. Наприклад, служби Windows Update завантажують оновлення, а служба Windows Audio відповідає за звук. Інші сервіси встановлюються сторонніми програмами. Наприклад, NVIDIA встановлює кілька сервісів у складі своїх графічних драйверів. За допомогою контекстного меню можна виконати: Пуск, Зупинити або Запустити знову службу.

Велика кількість служби має пов'язаний з ними процес «svchost.exe». Для отримання додаткової інформації про служби натисніть посилання «Відкрити служби» у нижній частині вікна.

Перелік служб Windows 10, до яких можна отримати доступ за допомогою комбінації "Win + R". Більшість з цих служб має інтерфейс користувача.

appwiz.cpl – видалення програм

calc – калькулятор

charmap – таблиця символів

chkdsk – утиліта для перевірки дисків  
cleanmgr – утиліта для очищення дисків  
cmd – командний рядок  
compmgmt.msc – управління комп'ютером  
control – панель управління  
control admintools – адміністрування  
control desktop – налаштування екрану/персоналізація  
control folders – властивості папок  
control fonts – шрифти  
control keyboard – властивості клавіатури  
control mouse – властивості миші  
control printers – пристрої та принтери  
control schedtasks – планувальник завдань  
desk.cpl – роздільна здатність екрану  
devmgmt.msc – диспетчер пристроїв  
dfrgui – дефрагментація дисків  
diskmgmt.msc – управління дисками  
dxdiag – засоби діагностики  
DirectX eventvwr.msc – перегляд подій  
explorer – провідник  
firewall.cpl – брандмауер  
Windows iexplore – браузер Internet Explorer  
inetcpl.cpl – властивості браузера  
Internet Explorer logoff – вийти з облікового запису користувача  
Windows magnify – лупа (збільшувальне скло)  
main.cpl – властивості миші  
migwiz – засіб перенесення даних  
Windows mmsys.cpl – налаштування звуку  
mrt – засіб видалення шкідливих програм  
msconfig – конфігурація системи  
msinfo32 – відомості про систему  
mspaint – графічний редактор Paint  
ncpa.cpl – мережеві підключення  
notepad – блокнот  
osk – екранна клавіатура  
perfmon – системний монітор  
powercfg.cpl – електроживлення  
psr – засіб запису дій по відтворенню неполадок  
regedit - редактор реєстру  
rrr - швидкий запуск  
Reg Organizer ([chemtable.com/ru/organizer.htm](http://chemtable.com/ru/organizer.htm)) shutdown – завершення роботи Windows  
sysdm.cpl – властивості системи  
syskey – захист БД облікових записів Windows  
taskmgr – диспетчер завдань

timedate.cpl – налаштування дати і часу  
 utilman – центр спеціальних можливостей  
 verifier – диспетчер перевірки драйверів  
 wab – адресна книга Windows  
 winver – версія Windows  
 wmpplayer – програвач Windows Media Player  
 write – редактор Wordpad  
 wscui.cpl – центр підтримки

Таблиця 3.1 Фрагмент переліку служб, перерахованих на вкладці "Сервіси"

Назва служби	Повна назва	Опис
xbgm	Xbox Game Monitoring	Моніторинг списку ігор. Якщо не використовується, доцільно відключити.
AJRouter	AllJoyn Router Service	Служба маршрутизатора AllJoyn: Перенаправляє повідомлення AllJoyn для локальних клієнтів AllJoyn. Якщо ця служба буде зупинена, клієнти AllJoyn, у яких немає своїх пов'язаних маршрутизаторів, не зможуть запуснитися. Запуск вручну.
ALG	Application Layer Gateway Service	Служба шлюзу рівня додатка. Дозволяє клієнтським додаткам використовувати динамічні порти TCP/UDP для взаємодії з відомими портами. Забезпечує підтримку стороннього протоколу для загального доступу до підключення до Інтернету. Якщо завершити процес, буде втрачений доступ до мережі. Відновлюється перезавантаженням.
AppIDSvc	Application Identity	Посвідчення програми: Визначає і перевіряє посвідчення додатки. Відключення даної служби унеможливило примусове застосування політики AppLocker.
Appinfo	Application Information	Відомості про програму. Забезпечує виконання інтерактивних додатків з додатковими адміністративними привілеями. Якщо ця служба буде зупинена, користувачі не зможуть запускати додатки з додатковими адміністративними привілеями, які можуть знадобитися для виконання потрібних для користувача завдань.
AppMgmt	Application Management	Управління додатками. Обробка запитів про установку, видалення і побудову списків для програм,

		встановлених через групову політику (для корпоративних мереж). При вимкненні цієї служби користувачі не зможуть встановлювати, видаляти і створювати списки програм, встановлених через групову політику. Якщо ця служба вимкнена, будь-які служби, які явно залежать від неї, не можуть бути запущені.
AppReadiness	AppReadiness	Підготовка додатків до використання при першому вході користувача на комп'ютер або додаванні нових додатків.
PeerDistSvc	BranchCache Stopped	Служба кешування мережеских даних, отриманих з локальної мережі. Виконує кешування цих даних, щоб прискорити доступ до перегляду та інших операцій: копіювання, переміщення, запуску, тощо. Не впливає на інші служби, не витрачає ресурси. Запускається вручну.
CoreMessagingRegistrar	CoreMessaging	Забезпечує зв'язок між компонентами системи (процеси та служби залежать один від одного, бібліотеки використовують одна одну).

Повний перелік служб та їх опис можна отримати на:  
<https://win10tweaker.pro/twikinarium/services/deviceassociationbroker>  
<http://batcmd.com/windows/10/services/xbgm/>

Таблиця 3.1 Фрагмент переліку особливих служб

Назва служби	Повна назва	Опис
DevicesFlowUserSvc	DevicesFlow	Віднайти та під'єднати пристрій
UserDataSvc	User Data Access	Служба доступу до структурованих даних користувача
MessagingService	MessagingService	Служба обміну повідомленнями між синхронізованими пристроями (наприклад, смартфон з комп'ютером)
WpnUserService	Windows Push Notifications User Service	Підтримка локальних і push-повідомлень
CDPUserSvc	Connected Devices Platform User Service	Служба платформи під'єднаних пристроїв користувача

Офіційний опис цих служб не співпадає з їх справжнім призначенням. Назви можуть бути з додаванням набору символів, які змінюються під час кожного пере завантаження ОС.

Наприклад, процес CDPUserSvc отримує доступ до призначених для користувача даних і веде обмін інформацією у зашифрованому вигляді з

серверами Microsoft. Яка саме інформація, не відомо, можливо, це персональні дані користувача Windows. Взаємодіє з наступними службами:

OneSyncSvc – синхронізує пошту, контакти, календар і інші призначені для користувача дані.

PimIndexMaintenanceSvc – індексує пошук по контактах на мобільних пристроях.

UnistoreSvc – відповідає за зберігання призначених для користувача даних, таких як контакти, календарі, повідомлення.

UserDataSvc – надає додаткам доступ до структурованих даних користувача.

Іншими словами, процес має доступ до будь-яких призначених для користувача даних, обмінюється якоюсь інформацією з серверами і ніяк не впливає на роботу операційної системи і додатків.

Перелік основних системних процесів ОС Windows:

svchost.exe – це загальна назва процесу, пов'язаного з системними функціями Windows, які запускаються з динамічних бібліотек. Під час запуску svchost.exe перевіряє реєстр функцій, щоб завантажити і запустити їх. Одночасно може бути запущено декілька екземплярів svchost.exe, залежно від того які служби запущені. Системна папка файлу svchost знаходиться в директорії C:\\Windows\\System32, під виглядом цього файлу в іншій теці може ховатися вірус або мережевий черв'як.

lsass.exe (Local Security Authentication Server). Процес відповідає за перевірку спроб авторизації у системі. Якщо стався успішний вхід до системи, процес створює маркер доступу користувача, а потім використовує його для запуску оболонки (explorer.exe).

Explorer.exe – графічна оболонка операційної системи Microsoft Windows, містить меню пуск, робочий стіл, панель інструментів і файловий менеджер.

sihost.exe (Shell Infrastructure Host) – запускає хост інфраструктури Shell, має завдання обробляти декілька графічних елементів інтерфейсу ОС, наприклад, відкривати панелі завдань і меню Пуск. Крім того, ця утиліта відображає програми в інтерфейсі Windows і керує певними функціями фонові поведінки, наприклад, зміною шпалер.

System – відповідає за роботу додатків у «фоновому» режимі, тобто без активного контролю з боку користувача.

ntkramp.exe – файл ядра ОС

wininit.exe (різновид Windows Start-Up Application) – відповідає за виконання процесу ініціалізації (запуску більшості постійно працюючих додатків у Windows). Запускає Lsm.exe (Local Session Manager), створює Services.exe (диспетчер управління службами або SCM).

dwm.exe - управляє відображенням вікон додатків, відповідає за візуальні і 3D ефекти та теми Windows, будує мініатюри вікон на панелі завдань, забезпечує підтримку дисплеїв і пристроїв з високою роздільною здатністю та ін.

smss.exe (Session Manager Subsystem) – відповідає за всі види діяльності, пов'язані з запуском, обробкою і закінчуючи призначеними для користувача сеансами в ОС Windows від версії 2000 і наступних. Викликає процедури Windows Logon (winlogon) і Client / Server Runtime Service (csrss).

services.exe – Диспетчер управління службами (Service Control Manager, SCM) – у Microsoft Windows (\Windows\System32\Services.exe) особливий системний процес, який реалізує технологію віддаленого виклику процедур (remote procedure call, RPC). Забезпечує створення, видалення, запуск і зупинку служб ОС.

winlogon.exe – відповідає за початок (logon) сеансу і завершення сеансу (logoff) користувача. Процес активується тільки після натискання користувачем клавіш CTRL + ALT + DEL і демонструє діалогове вікно для введення пароля. Файл WINLOGON.

csrss.exe – відповідає за консольні (режим командного рядка) програми, процес вимкнення, запуск іншого важливого процесу – conhost.exe і інші критичні функції системи.

conhost.exe – обробляє консольні вікна в останніх версіях Windows, вирішує одну з фундаментальних проблем попередніх версій Windows, яка проявлялася при управлінні консольними вікнами і порушувала роботу у режимі перетягування об'єктів «drag & drop».

Системні фонові процеси:

RuntimeBroker.exe – один з основних процесів ядра ОС. Призначений для визначення та управління дозволами для «UWP-додатків». Дозволяє додатку отримати доступ до місцезнаходження або мікрофона. Постійно працює у фоновому режимі і активується при запуску будь-якої програми з «Windows Store». Даний процес працює як посередник, який запускає встановлені «UWP-додатки» з налаштуваннями безпеки і конфіденційності.

ApplicationFrameHost.exe – служба відображення певних програм у кадрах. Процес Host Frame Host призначений для відображення традиційних додатків Windows у кадрах незалежно від пристрою, який використовують.

ctfmon.exe – контролює всі активні вікна і забезпечує підтримку сервісу вводу тексту для розпізнавання мови, розпізнавання рукописних символів, клавіатури, перекладача та інших альтернативних технологій вводу.

SecurityHealthService.exe – системна служба, що відповідає у Windows 10 за роботу Центру безпеки. Управляється Системою, завершення через Диспетчер завдань не передбачено.

spoolsv.exe – процес, що забезпечує виведення на друк з використанням принтера та інших подібних пристроїв. Не є особливо важливим, може бути завершений з Диспетчера завдань або вимкнений у службах.

wuauclet.exe – процес, який реалізує Microsoft's AutoUpdate (функцію автоматичного оновлення) для різних версій Windows. Вона працює у фоновому режимі, зазвичай в режимі очікування, але періодично опитує сайт Microsoft, щоб перевірити наявність оновлень, установка яких може знадобитися.

hkcmd.exe – надає доступ до спеціальних гарячих клавіш, що забезпечують параметри конфігурації для вбудованих графічних контролерів на визначених чіпсетах Intel. Встановлюється автоматично разом з драйверами для чіпсетів Intel 810 і 815, і хоча не є основним, рекомендується не вимикати його з метою забезпечення сталої роботи системи.

### 3.3 Контрольні завдання.

Отримати перелік служб для процесу svchost.exe, який забезпечить прослуховування аудіо записів.

Порівняти час роботи у режимі ядра і у режимі користувача для запам'ятовуючого пристрою USB для усієї групи лічильників.

Серед загального переліку встановлених драйверів пристроїв Вашої системи знайдіть дані про драйвер для USB HID-сумісного пристрою.

Запустіть процес Microsoft Word і визначте для нього: кількість оперативної пам'яті; сервіси; кількість операцій читання, виконаних процесом з моменту його запуску; кількість активних потоків у процесі; властивості процесу; визначити його пріоритет.

Для будь-якого додатку задати автозавантаження.

З'ясуйте, які програми (з тих, що завантажуються автозавантаженням) на Вашому комп'ютері є "полегшеними", а які – "важкими".

Завершити процес Explorer.exe, а потім запустити його за допомогою командного рядка Диспетчера завдань.

Використовуючи одну зі служб переналаштувати властивості миші.