

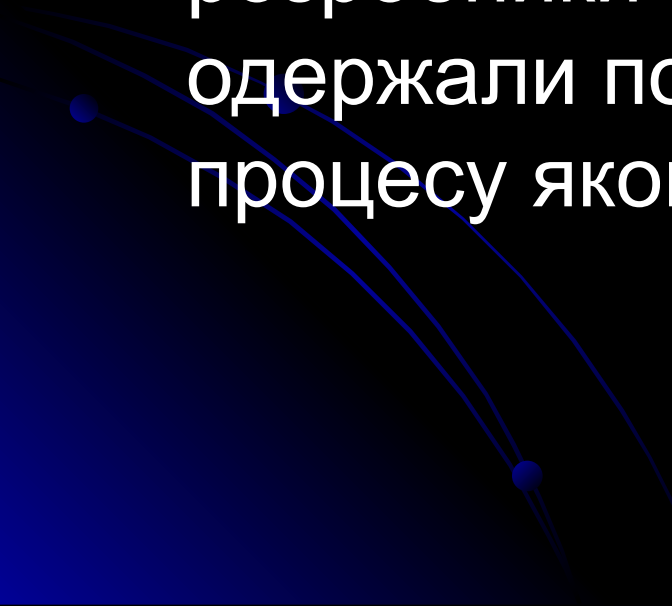
# Системне програмування

Лекція № 6

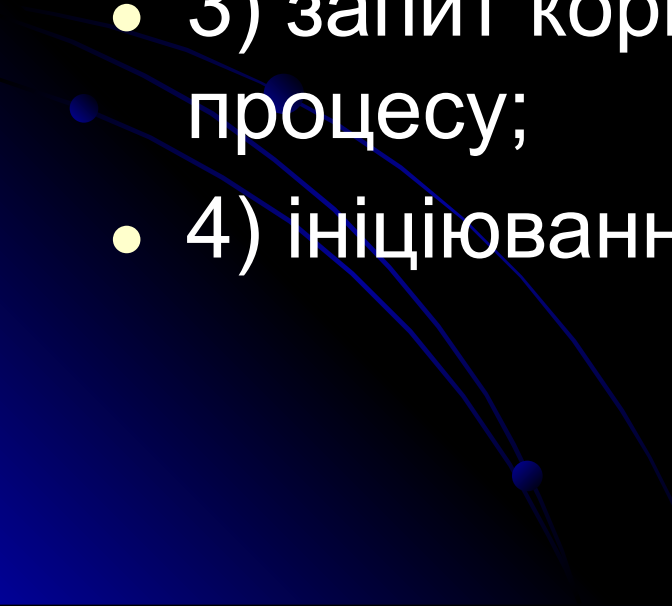
Лектор Артамонов Є.Б.



# Поняття процесу

- Процес – це абстрактне поняття, що описує роботу програми. Все інше базується на цьому понятті, тому представляється вкрай важливим, щоб розробники операційних систем одержали повне подання про концепції процесу якомога раніше.
- 

# Створення процесу

- 1) ініціалізація системи;
  - 2) виконання виданого працюючим процесом системного запиту на створення процесу;
  - 3) запит користувача на створення процесу;
  - 4) ініціювання пакетного завдання.
- 

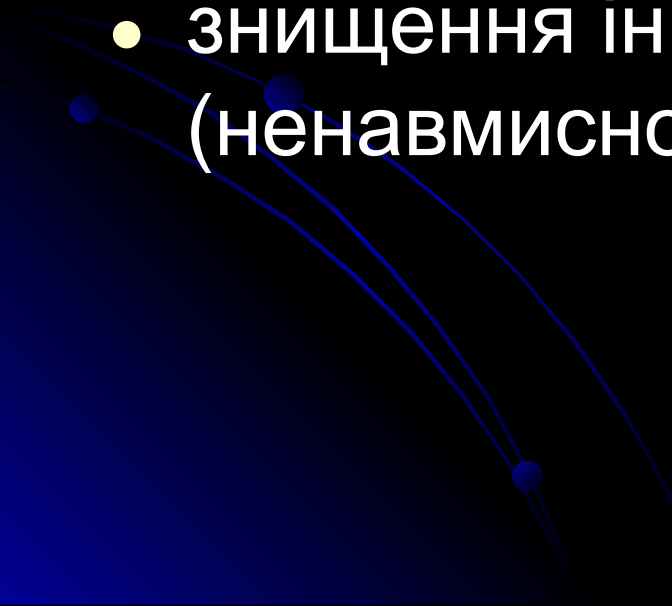
# Створення процесу

- Основні функції: `CreateProcess`, `CreateProcessAsUser` (для Win NT/2000) і `CreateProcessWithLogonW` (починаючи з Win2000).
- Етапи:
  - відкривається файл образу (EXE).
  - якщо виконуваний файл не являється Win32 додатком, то шукається образ підтримки (support image) для запуску цієї програми.

# Етапи запуску win32 процесу

- Створюється об'єкт Win32 "процес".
- Створюється первинний потік (стек, контекст і об'єкт "потік").
- Підсистема Win32 повідомляється про створення нового процесу і потоку.
- Починається виконання первинного потоку.
- У контексті нового процесу і потоку ініціалізувався адресний простір (наприклад, завантажуються необхідні DLL) і починається виконання програми.

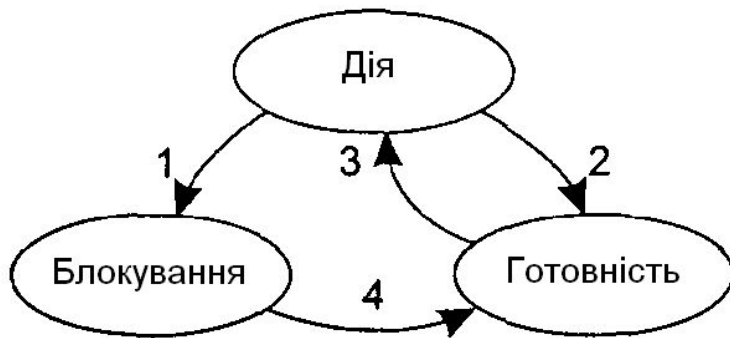
# Завершення процесу

- звичайний вихід (навмисно);
  - вихід помилково (навмисно);
  - вихід по непоправній помилці (ненавмисно);
  - знищення іншим процесом (ненавмисно).
- 

# Стани процесів

- працюючий (у цей конкретний момент використовує процесор);
- готовий до роботи (процес тимчасово припинений, щоб дозволити виконуватися іншому процесу);
- заблокований (процес не може бути запуснений перш, ніж відбудеться якась зовнішня подія).

# Стани процесів



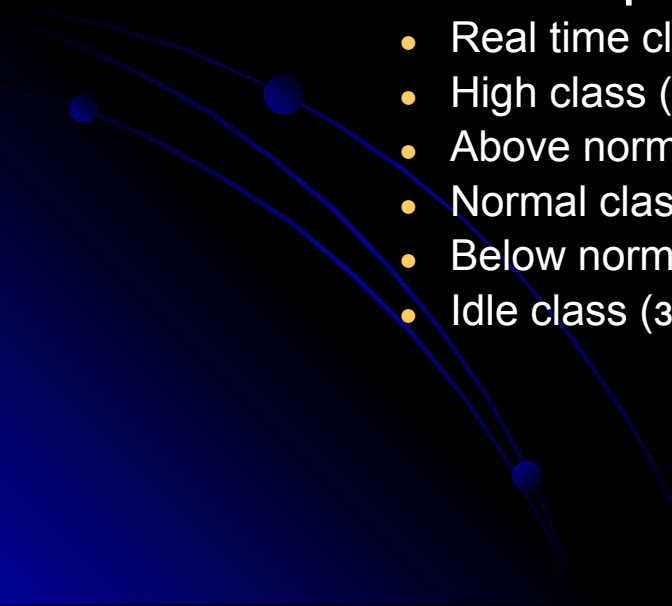
1. Процес блокується, очікуючи нових даних
2. Планувальник вибирає інший процес
3. Планувальник вибврає цей процес
4. Доступні вхідні данні



# Деякі поля типового елемента таблиці процесів

Керування процесом	Керування пам'яттю	Керування файлами
Регістри	Вказівник на текстовий сегмент	Корінний каталог
Лічильник команд	Вказівник на сегмент	Робочий каталог
Слово стану програми	Вказівник на сегмент даних	Дескриптори файлу
Вказівник стека	стека	Ідентифікатор користувача
Стан процесу		Ідентифікатор групи
Пріоритет		
Параметри планування		
Ідентифікатор процесу		

# Пріоритети процесів

- У Windows існує 32 рівні пріоритету, від 0 до 31. Вони поділяються на два блоки від 31 – 16 – пріоритети реального часу; від 15 - 1 динамічні рівні; 0 - системний пріоритет, зарезервований для потоку обнулення сторінок (zero-page thread).
  - При створенні процесу, йому призначається один з шести класів пріоритетів:
    - Real time class (значення 24);
    - High class (значення 13);
    - Above normal class (значення 10),
    - Normal class (значення 8),
    - Below normal class (значення 6),
    - Idle class (значення 4).
- 

# Пріоритети потоків

- Пріоритет кожного потоку (базовий пріоритет потоку) складається з пріоритету його процесу і відносного пріоритету самого потоку.
- Є сім відносних пріоритетів потоків:
  - Normal: такий же як і у процесу;
  - Normal: +1 до пріоритету процесу;
  - Below normal: -1;
  - Highest: +2;
  - Lowest: -2;
  - Time critical: встановлює базовий пріоритет потоку для Real time класу в 31, для решти класів в 15.
  - Idle: встановлює базовий пріоритет потоку для Real time класу в 16, для решти класів в 1.

# Інтерактивні та фонові процеси

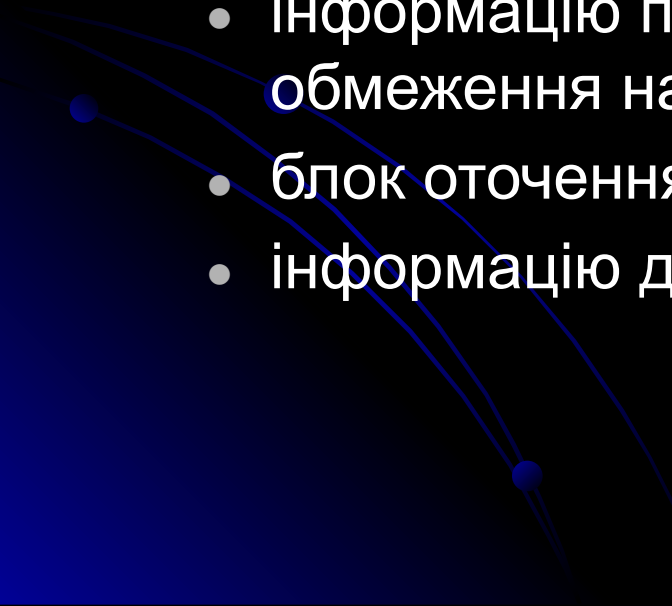
- *Інтерактивні процеси* взаємодіють із користувачами безпосередньо, приймаючи від них дані, введені за допомогою клавіатури, миші тощо. Прикладом інтерактивного процесу може бути процес текстового редактора або інтегрованого середовища розробки.
- *Фонові процеси* із користувачем не взаємодіють безпосередньо. Зазвичай вони запускаються під час старту системи і чекають на запити від інших застосувань. Деякі з них (системні процеси) підтримують функціонування системи (реалізують фонове друкування, мережні засоби тощо), інші виконують спеціалізовані задачі (реалізують веб-сервери, сервери баз даних тощо). Фонові процеси також називають службами (services, у системах лінії Windows XP) або демонами (daemons, в UNIX).

# Структури даних процесу

- У режимі користувача доступним є *блок оточення процесу* (process environment block, PEB), що перебуває в адресному просторі цього процесу.

EPROCESS і KPROCESS, на відміну від PEB, доступні тільки із привілейованого режиму.

# Структури даних процесу

- Керуючий блок процесу містить такі основні елементи:
    - блок процесу ядра (KPROCESS);
    - ідентифікаційну інформацію;
    - інформацію про адресний простір процесу;
    - інформацію про ресурси, доступні процесу, та обмеження на використання цих ресурсів;
    - блок оточення процесу (PEB);
    - інформацію для підсистеми безпеки.
- 

# Ідентифікація інформації

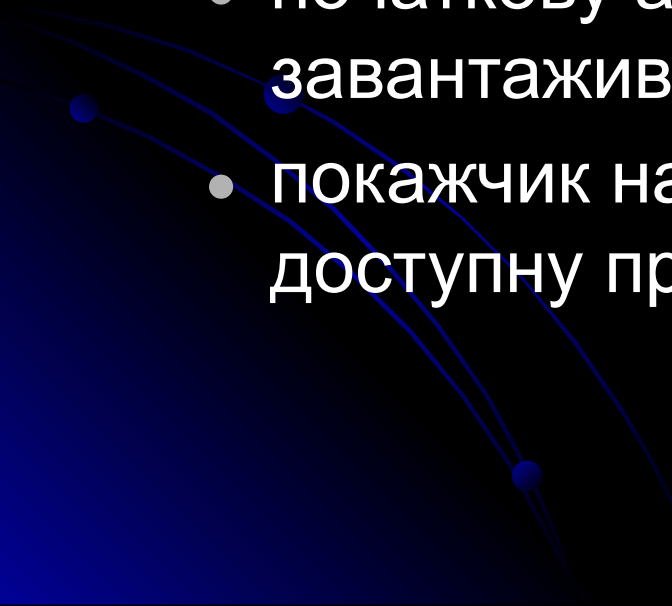
- ідентифікатор процесу (pid);
- ідентифікатор процесу, що створив цей процес (незважаючи на те, що Windows XP не підтримує відносини «предок-нащадок» автоматично, вони можуть бути задані програмним шляхом, тобто нащадок може сам призначити собі предка, задавши цей ідентифікатор);
- ім'я завантаженого програмного файлу.

# Блок процесу ядра

- містить усю інформацію, що належить до потоків цього процесу:
  - покажчик на ланцюжок блоків потоків ядра, де кожний блок відповідає потоку;
  - базову інформацію, необхідну ядру системи для планування потоків (ця інформація буде успадкована потоками, пов'язаними із цим процесом).



# Блок оточення процесу

- містить інформацію про процес, яка призначена для доступу з режиму користувача:
    - початкову адресу ділянки пам'яті, куди завантажився програмний файл;
    - покажчик на динамічну ділянку пам'яті, доступну процесу.
- 

# Методи маскування і виявлення процесів в операційній системі Windows



# Програмне забезпечення TaskInfo

The screenshot displays the TaskInfo application window. At the top, it shows system status: 5.87% TaskInfo -- Not Registered 0 Days. Below the menu bar, there are several status indicators: Vite=47%, Ram=37%, Swp=8%, MMapiO<10M, and FieldO<1M. A central graph shows various system metrics over time. Below the graph is a process list table with columns for Process, PID, % CPU, % K CPU, and CPU. The list includes various system services and applications, with TaskInfo Application at the bottom showing 0.78% CPU usage. To the right of the process list is a detailed system statistics panel with tabs for System, CPU, All Open Files, Connections, Drivers, OS, and RAS. The System tab is active, showing metrics like CPU Clock MHz (3 679), % CPU (5.87%), and % Idle Pri Threads (94.13%). Below the statistics panel is a General tab showing system information such as CMD, Curr Dir, Path, User Name, and various resource usage statistics. In the bottom right corner, a small dialog box titled 'Too Many GDI Objects' is visible, showing an Alert Level of '< 4 000' and a GDI Objects Number of 4 281.

Process	PID	% CPU	% K CPU	CPU
+ UpdateChecker Module	1 600			
+ Lingvo Launcher	1 624			
+ Point32.exe	1 656			
+ DIHelper Application	1 680			
+ AcroTray	1 880			
+ TrueImage	1 900			
+ Acronis Scheduler Helpe	1 908			
+ Kaspersky Anti-Virus	1 764			
+ CTF Loader	1 956			
+ ATI Tray Tools	356			
+ DAEMON Tools main.ap	496			
+ Logitech Desktop Messe	644			
+ GammaTray MFC ??? ???	732			
+ Launchy	760			
+ Logitech SetPoint Event	772			
+ ABBYY network license t	1 228			
+ Logitech KHAL Main Pro	2 000			
+ Acronis Scheduler 2	2 244			
+ Apache HTTP Server	2 232			
+ Microsoft ASP.NET State	2 336			
+ System Level Service Uti	2 372			
+ Kaspersky Anti-Virus	2 424			
+ Bonjour Service	2 496			
+ Creative Service for CDR	2 560			
+ Machine Debug Manage	2 860			
+ mysqld-nt.exe	3 212			
+ Apache HTTP Server	3 252			
+ SMSvcHost.exe	3 292			
+ D&O Defrag Agent	2 164			
+ PnkBstA.exe	2 528			
+ Remote control tool	2 832			
+ SoundMAX service agen	2 072			
+ Generic Host Process for	2 160			
+ Telnet	1 580			
+ WMDM PMSP Service	2 082			
+ Activation Licensing Ser	4 652			
+ Application Layer Gatew	5 328			
+ Generic Host Process for	4 372			
+ speedfan.exe	4 480	0.39%	0.39%	
+ ICQ Library	4 832	0.39%		
+ Opera Internet Browser	6 136	1.95%	1.95%	
+ Microsoft Office Word	4 416			
+ TaskInfo Application	4 640	0.78%		

System	CPU	All Open Files	Connections	Drivers	OS	RAS
CPU Clock MHz	3 679					
% CPU	5.87%	% Idle Pri Threads			94.13%	
CPUs Number	2	Queue for CPU			2	
Processes	65	Threads			881	
Thread Sw/s	12 383	HW Int/s			1 285	
Total Ph KB	2 095 852	Free Ph KB			1 313 288	
File Cache KB	223 100	File cache peak KB			274 244	
Free Vnt KB	2 150 720	Committed KB			1 895 972	
Paged Pool KB	83 876	NonPaged Pool KB			46 532	
Max Swap KB	2 095 104	Swap in Use KB			189 040	
Page Faults/s	518					
Page Ins KB/s	0	Page Outs KB/s			16	
File Read KB/s	1	File Write KB/s			33	
File Reads/s	7	File Writes/s			8	
Client Read KB/s	0	Client Write KB/s			0	
Srv Transmit KB/s	0	Srv Receive KB/s			0	

General	Modules	Files	Handles	Connections	Env	Image Info	Thread(s)
CMD		= "C:\Program Files\Opera\Opera.exe"					
Curr Dir		= C:\Documents and Settings\Алексея\					
Path		= C:\Program Files\Opera\Opera.exe					
User Name		= REDLINE \Алексея					
PID/Parent PID		= 6136 / 976					
Started by		= C:\WINDOWS\Explorer.EXE					
Virtual KB		Curr = 188 572 Peak = 236 108					
Working Set KB		Curr = 36 472 Peak = 78 972					
Page File KB		Curr = 68 168 Peak = 72 856					
System Pool KB		Paged = 81 Nonpaged = 27					
Private KB		= 68 168					
Handles Count		= 329					
Faults Count		= 189 292					
Objects		= USER = 150 GDI = 883					
Windows		= 83					
Reads		= 10 097 Read KB = 16 084					
Writes		= 147 746 Write KB = 18 346					
Other IOs		= 48 911 Other KB = 169 733					

**Too Many GDI Objects**

Alert Level < 4 000

GDI Objects Number 4 281

[Alerts Configuration](#) [Help](#)

# Програмне забезпечення Process Explorer

The screenshot displays the Process Explorer application window. The main window shows a list of processes with columns for Process, PID, CPU, Description, and Company Name. The process explorer.exe is highlighted in blue. A properties dialog box for explorer.exe is open, showing details such as Image File (C:\WINDOWS\Explorer.EXE), Command line, and User (REDLINE\Алексей).

Process	PID	CPU	Description	Company Name
System Idle Process	0	0.00	System Idle Process	
System	4	0.00	System	
smss.exe	936	0.00	Диспетчер сеанса Windo...	Корпорация Майкрософт
csrss.exe	992	0.00	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	1020	0.00	Программа входа в систе...	Корпорация Майкрософт
services.exe	1064	0.76	Приложение служб и конт...	Корпорация Майкрософт
ati2evxx.exe	1268	0.00	ATI External Event Utility EX...	ATI Technologies Inc.
svchost.exe	1284	0.00	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	1356	0.00	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	1728	0.00	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	1784	0.00	Generic Host Process for WL...	Microsoft Corporation
svchost.exe	368	0.00	Generic Host Process for WL...	Microsoft Corporation
spoolsv.exe	592	0.00	Spooler SubSystem App	Microsoft Corporation
NetworkLicens...	1228	0.00	ABBYY network license server	ABBYY (BIT Software)
schedul2.exe	2244	0.00	Acronis Scheduler 2	Acronis
httpd.exe	2232	0.00	Apache HTTP Server	Apache Software Foundati...
httpd.exe	3252	0.00	Apache HTTP Server	Apache Software Foundati...
aspnet_state.exe	2336	0.00	Microsoft ASP.NET State Se...	Microsoft Corporation
AdskScSrv.exe	2372	0.00	System Level Service Utility	Autodesk
avp.exe	2424	0.00	Kaspersky Anti-Virus	Kaspersky Lab
mDNSRespon...	2496	0.00	Bonjour Service	Apple Computer, Inc.
CTSVCCDA.EXE	2560	0.00	Creative Service for CDRDM...	Creative Technology Ltd
mdm.exe	2860	0.00	Machine Debug Manager	Microsoft Corporation
mysqld-nt.exe	3212	0.00	MySQL Database Server	MySQL AB
SMSvcHost.exe	3232	0.00	SMSvcHost.exe	Microsoft Corporation
nodag.exe	2164	5.30	O&O D&O Diagrag Agent	O&O Software GmbH
PnkBstrA.exe	2528	0.00	Remote control tool	Stardock Systems, Inc
_server.exe	2832	0.00	Remote control tool	Stardock Systems, Inc
SMAgent.exe	2072	0.00	SoundMAX service agent co...	Analog Devices, Inc.
svchost.exe	2160	0.00	Generic Host Process for WL...	Microsoft Corporation
lntsvr.exe	1580	0.00	Telnet	Корпорация Майкрософт
MsPMSPSv.exe	2092	0.00	WMDM PMSP Service	Microsoft Corporation
FNPLicensingS...	4652	0.00	Activation Licensing Service	Macrovision Europe Ltd.
alg.exe	5328	0.00	Application Layer Gateway S...	Microsoft Corporation
svchost.exe	4372	0.00	Generic Host Process for WL...	Microsoft Corporation
lsass.exe	1076	0.00	LSA Shell (Export Version)	Microsoft Corporation
ati2evxx.exe	2024	0.00	ATI External Event Utility EX...	ATI Technologies Inc.
wbload.exe	668	0.00	WindowBlinds	Stardock Systems, Inc
explorer.exe	976	0.00	Проводник	Корпорация Майкрософт
SMmaxPNP.exe	1484	0.00	SMmaxPNP MFC Application	Analog Devices, Inc.
CTSysVol.exe	1504	0.00	CTSysVol.exe	Creative Technology Ltd
CTDVDDT.exe	1512	0.00	CTDVDDT	Creative Technology Ltd
juchecked.exe	1556	0.00	UpdateChecker Module	SAMSUNG ELECTRONICS
jucheck.exe	1600	0.00	UpdateChecker Module	SAMSUNG ELECTRONICS
SMSTray.exe	1568	0.00	SMSTray.exe	SAMSUNG ELECTRONICS
LvAgent.exe	1624	0.00	Lingvo Launcher	ABBYY (BIT Software)
point32.exe	1656	0.00	Point32.exe	Microsoft Corporation
CTHELPER.EXE	1680	0.00	CHelper Application	Creative Technology Ltd
Acrotray.exe	1880	0.00	AcroTray	Adobe Systems Inc.
TrueImageMonitor.exe	1900	0.00	TrueImage	Acronis
schedlnp.exe	1908	0.00	Acronis Scheduler Helper	Acronis

explorer.exe:976 Properties

Image File: Проводник (Not verified) Корпорация Майкрософт  
Version: 6.00.2900.5512  
Time: 14.04.2008 21:40  
Path: C:\WINDOWS\Explorer.EXE  
Command line: C:\WINDOWS\Explorer.EXE  
Current directory: C:\Documents and Settings\Алексей\

Parent: <Non-existent Process>(952)  
User: REDLINE\Алексей  
Started: 9:40:41 25.05.2008  
Comment: Data Execution Protection (DEP) Status: Disabled

OK Cancel

# Програмне забезпечення Codestuff Starter

Starter (Windows XP Professional)

File Process Configuration Help

Exit New Edit Terminate Refresh Launch Properties Options About

Startups Processes Services

Process	PID	Mem usage	Executable	Priority	Page fault count	Mem usage (pe...)	Paged pool (peak)	Paged pool	Nonpaged pool (peak)	Nonpaged po...
Lvagent.exe	1624	4 112 384	C:\Program Files\ABBYY Lingvo 11 S...	20 (Normal)	1 310	4 112 384	34 704	30 064	3 272	2 6...
point32.exe	1656	6 184 960	C:\Program Files\Microsoft IntelliPoint...	20 (Normal)	2 307	6 184 960	42 688	38 548	4 312	3 7...
CTHELPER.EXE	1680	10 887 168	C:\WINDOWS\CTHELPER.EXE	20 (Normal)	7 161	10 899 456	59 020	44 900	9 008	7 0...
svchost.exe	1728	33 419 264	C:\WINDOWS\System32\svchost.exe	20 (Normal)*	26 064	37 298 176	169 160	165 728	103 248	95 9...
avp.exe	1764	3 162 112	C:\Program Files\Kaspersky Lab\Kas...	20 (Normal)	17 945	12 922 880	58 180	54 016	19 296	16 8...
svchost.exe	1784	4 116 480	C:\WINDOWS\System32\svchost.exe	20 (Normal)	5 226	4 145 152	35 356	31 428	9 088	5 0...
Acrotray.exe	1880	12 763 136	D:\Programs\Acrobat 8.0\Acrobat\A...	20 (Normal)	10 069	20 500 480	89 324	49 352	11 040	6 9...
TrueImageMonitor...	1900	7 254 016	C:\Program Files\Acronis\TrueImage\...	20 (Normal)	2 958	7 254 016	44 044	36 120	5 352	4 2...
schedhlp.exe	1908	6 770 688	C:\Program Files\Common Files\Acro...	20 (Normal)	2 737	6 770 688	43 576	35 324	5 112	3 8...
ctfmon.exe	1956	7 438 336	C:\WINDOWS\System32\ctfmon.exe	20 (Normal)	4 732	7 438 336	46 460	38 968	6 112	5 3...
KHALMNPR.EXE	2000	7 892 992	C:\Program Files\Common Files\Logit...	20 (Normal)	2 964	7 892 992	43 648	38 024	6 288	5 6...
Ah2evwx.exe	2024	3 448 832	C:\WINDOWS\System32\Ah2evwx.exe	20 (Normal)*	941	3 502 080	27 012	24 748	3 680	3 0...
SMAgent.exe	2072	1 982 464	C:\Program Files\Analog Devices\So...	20 (Normal)*	501	1 982 464	30 320	23 840	2 312	1 8...
MsPMSP5v.exe	2092	1 757 184	C:\WINDOWS\System32\MsPMSP5v...	20 (Normal)*	433	1 757 184	15 820	15 820	2 152	1 7...
svchost.exe	2160	5 173 248	C:\WINDOWS\System32\svchost.exe	20 (Normal)*	1 543	5 242 880	39 208	38 560	5 696	4 0...
oodag.exe	2164	6 209 536	C:\WINDOWS\System32\oodag.exe	20 (Normal)*	5 810	6 209 536	33 784	30 612	35 632	34 5...
schedu2.exe	2244	1 945 600	C:\Program Files\Common Files\Acro...	20 (Normal)*	483	1 970 176	18 148	17 948	2 568	1 9...
httpd.exe	2292	9 998 336	F:\Apache 2.2\bin\httpd.exe	20 (Normal)*	3 596	9 998 336	35 924	35 428	36 320	35 3...
asprnl_state.exe	2336	3 616 768	C:\WINDOWS\Microsoft.NET\Frame...	20 (Normal)	893	3 616 768	26 168	26 152	36 168	36 0...
AdskScSrv.exe	2372	1 363 968	C:\Program Files\Common Files\Auto...	20 (Normal)*	346	1 363 968	13 788	13 788	2 216	1 8...
avp.exe	2424	19 087 360	C:\Program Files\Kaspersky Lab\Kas...	20 (Normal)	1 092 123	75 386 880	95 184	91 724	117 696	90 4...
mdNSResponder...	2496	3 817 472	C:\Program Files\Bonjour\mdNSRes...	20 (Normal)*	1 092	4 239 360	28 684	25 332	9 088	5 4...
PrkBstA.exe	2528	2 756 608	C:\WINDOWS\System32\PrkBstA.e...	20 (Normal)*	693	2 756 608	31 948	26 568	3 072	2 8...
CTsvcCDA.exe	2560	1 486 848	C:\WINDOWS\System32\CTsvcCDA...	20 (Normal)*	373	1 486 848	13 796	13 500	2 256	1 4...
l_server.exe	2832	5 591 040	C:\WINDOWS\System32\l_server.exe	20 (Normal)*	4 162	5 591 040	34 960	30 404	5 896	3 8...
mdm.exe	2860	3 383 296	C:\Program Files\Common Files\Micro...	20 (Normal)*	1 127	3 551 232	43 468	26 432	3 672	2 8...
mysqld-nt.exe	3212	71 581 696	C:\Program Files\MySQL\MySQL Ser...	20 (Normal)*	40 576	129 515 520	57 980	57 420	22 264	11 8...
Starter.exe	3248	11 628 544	E:\Progs\Starter\Starter.exe	20 (Normal)	8 521	11 739 136	47 964	43 576	7 040	6 5...
httpd.exe	3252	11 468 800	F:\Apache 2.2\bin\httpd.exe	20 (Normal)*	3 945	11 468 800	39 012	39 012	24 864	24 5...
SM5svchost.exe	3292	12 857 344	C:\WINDOWS\Microsoft.NET\Frame...	20 (Normal)	3 268	12 857 344	80 196	80 164	4 508	3 7...
mspaint.exe	4104	34 418 688	C:\WINDOWS\System32\mspaint.exe	20 (Normal)	553 834	63 356 928	68 708	48 272	8 240	6 7...
svchost.exe	4372	3 784 704	C:\WINDOWS\System32\svchost.exe	20 (Normal)*	963	3 792 896	35 356	33 484	10 872	9 7...
WINWORD.EXE	4416	51 699 712	C:\Program Files\Microsoft Office\Offi...	20 (Normal)	210 973	60 497 920	262 212	238 908	19 880	18 8...
speedfan.exe	4480	3 461 120	C:\Program Files\SpeedFan\speedfa...	20 (Normal)	7 461	11 902 976	50 212	48 988	8 336	6 7...
FNPLicensingSer...	4652	2 744 320	C:\Program Files\Common Files\Macr...	20 (Normal)*	957	3 022 848	16 660	16 620	4 488	2 2...
ICQ.exe	4832	18 804 736	C:\Program Files\ICQ6\ICQ.exe	20 (Normal)	354 063	74 153 984	143 140	135 148	33 968	27 4...
alg.exe	5328	3 817 472	C:\WINDOWS\System32\alg.exe	20 (Normal)	987	3 829 760	36 792	36 192	6 216	5 2...
Opera.exe	6136	65 871 872	C:\Program Files\Opera\Opera.exe	20 (Normal)	412 689	80 867 328	127 368	83 028	86 492	29 2...

Module (26)	Handle	Size	Full Path
COMCTL32.dll	773C0000	1 060 864	C:\WINDOWS\WinSxS\X86_Microsoft.Windo...
GDI32.dll	77F10000	299 008	C:\WINDOWS\System32\GDI32.dll
IMM32.DLL	76360000	118 784	C:\WINDOWS\System32\IMM32.DLL
kernel32.dll	7C800000	1 015 808	C:\WINDOWS\System32\kernel32.dll

Lingvo Launcher / 11.0.0.291 / Lingvo / ABBYY (BIT Software) / Copyright © 2004 ABBYY Software Ltd.

0,78% | 1,56% | 0,00% | 1,268,920,920 Processes: 66



# Програмне забезпечення System Observer

System Observer v1.0

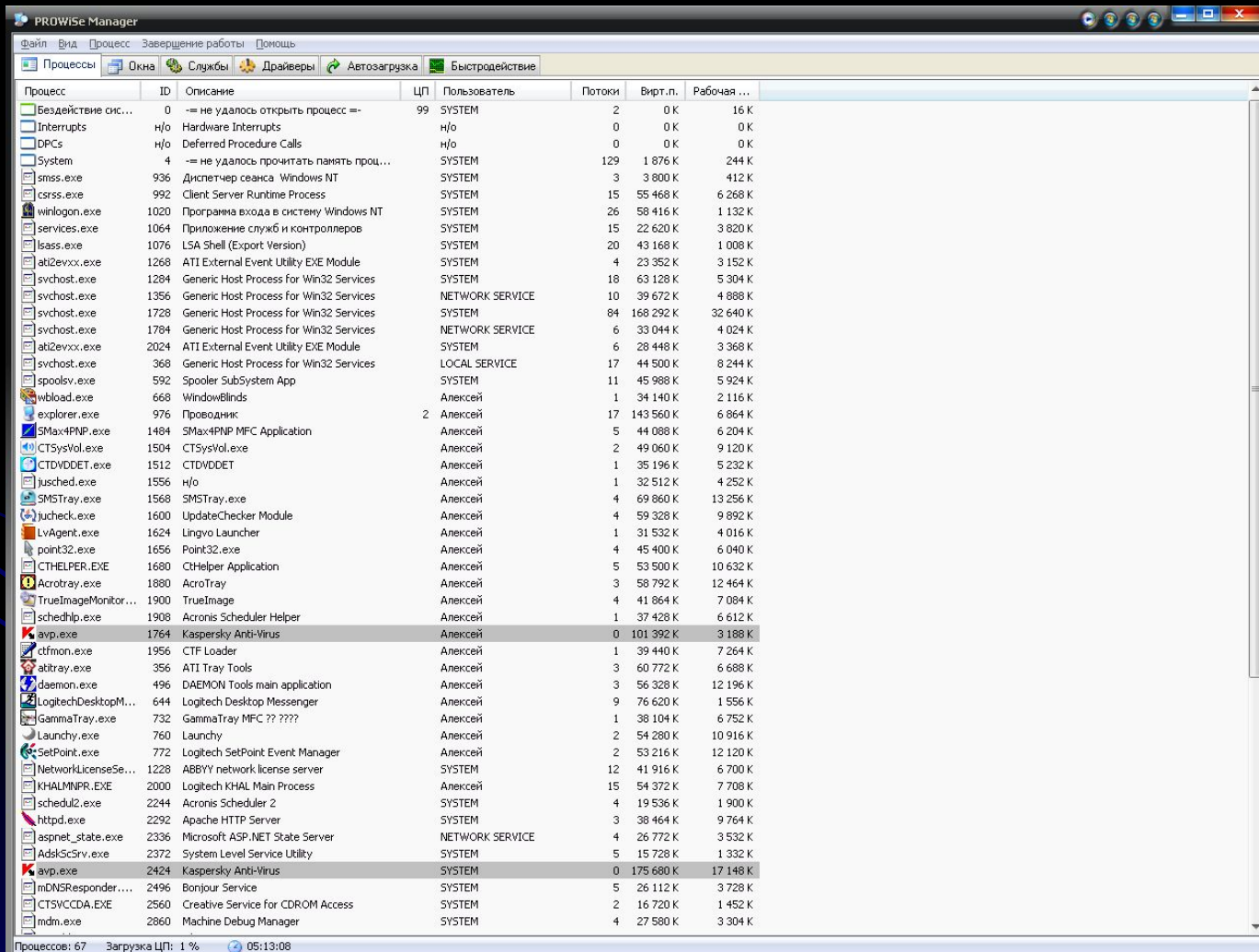
Файл Параметри Вид Завершение работы Справка

ЦП: 4.7%

Приложение	ИД	Название	ЦП	Физ. память	История ЦП	вание памяти	Вирт.п.	Баз.пр.
multiWeather	1140	WINWORD.EXE		50 824 КБ		62 564 КБ	31 492 КБ	Средний
2 Разговоры - Suffering	03FC	winlogon.exe		880 КБ		19 776 КБ	7 616 КБ	Высокий
E:\Progs\Starter	029C	wload.exe		2 116 КБ		3 272 КБ	1 500 КБ	Средний
Безымянный - Paint	076C	TrueImageMonitor.exe		7 084 КБ		7 084 КБ	2 860 КБ	Средний
Документ1 - Microsoft Word	062C	tlntsvr.exe		3 024 КБ		3 032 КБ	628 КБ	Средний
Загрузки - Opera	0004	System		244 КБ		2 832 КБ	0 КБ	Средний
	1114	svchost.exe		3 696 КБ		3 704 КБ	1 652 КБ	Средний
	0870	svchost.exe		5 064 КБ		5 124 КБ	2 888 КБ	Средний
	0170	svchost.exe		8 236 КБ		8 332 КБ	5 396 КБ	Средний
	06F8	svchost.exe		3 940 КБ		4 048 КБ	1 560 КБ	Средний
	06C0	svchost.exe		32 740 КБ		36 424 КБ	19 148 КБ	Средний
	054C	svchost.exe		4 880 КБ		4 908 КБ	1 964 КБ	Средний
	0504	svchost.exe		5 304 КБ		5 380 КБ	3 112 КБ	Средний
	0250	spoolsv.exe		5 924 КБ		6 656 КБ	3 328 КБ	Средний
	1180	speedfan.exe		3 396 КБ		11 624 КБ	4 764 КБ	Средний
	0930	SO.exe	4.69	8 660 КБ		8 660 КБ	5 448 КБ	Высокий
	0CDC	SMsvchost.exe		12 556 КБ		12 556 КБ	17 736 КБ	Средний
	0620	SMSTray.exe		13 256 КБ		13 272 КБ	5 296 КБ	Средний
	03A8	sms.exe		412 КБ		480 КБ	172 КБ	Выше средн...
	05CC	SMax4PMP.exe		6 188 КБ		6 192 КБ	3 188 КБ	Средний
	0818	SMAgent.exe		1 936 КБ		1 936 КБ	612 КБ	Средний
	0304	SetPoint.exe		12 120 КБ		17 864 КБ	5 796 КБ	Средний
	0428	services.exe		3 780 КБ		3 840 КБ	1 832 КБ	Средний
	08C4	schedul2.exe		1 900 КБ		1 924 КБ	596 КБ	Средний
	0774	schedhlp.exe		6 612 КБ		6 612 КБ	2 540 КБ	Средний
	0810	r_server.exe		5 460 КБ		5 460 КБ	2 416 КБ	Средний
	0678	point32.exe		6 040 КБ		6 040 КБ	3 204 КБ	Средний
	09E0	PrintSpA.exe		2 692 КБ		2 692 КБ	1 832 КБ	Средний
	17F8	Opera.exe		61 424 КБ		78 972 КБ	73 588 КБ	Средний
	0874	oodag.exe		6 064 КБ		6 064 КБ	4 068 КБ	Средний
	04CC	NetworkLicenseServer.exe		6 700 КБ		6 704 КБ	3 436 КБ	Средний
	0C8C	mysqld-nt.exe		69 904 КБ		126 480 КБ	1 254 008 КБ	Средний
	082C	MsRMSPSv.exe		1 716 КБ		1 716 КБ	512 КБ	Средний
	1008	nspaint.exe		33 656 КБ		61 872 КБ	26 504 КБ	Средний
	09C0	mDNSResponder.exe		3 728 КБ		4 140 КБ	1 176 КБ	Средний
	082C	mdm.exe		3 304 КБ		3 468 КБ	1 004 КБ	Средний
	0658	LvAgent.exe		4 016 КБ		4 016 КБ	1 416 КБ	Средний
	0434	lsass.exe		1 144 КБ		6 564 КБ	3 832 КБ	Средний
	0284	LogitechDesktopMesseng...		1 784 КБ		14 888 КБ	11 316 КБ	Средний
	02F8	Launchy.exe		10 980 КБ		11 000 КБ	6 348 КБ	Средний
	07D0	KHALMNP.R.EXE		7 708 КБ		7 708 КБ	4 372 КБ	Средний
	0614	jusched.exe		4 252 КБ		4 260 КБ	1 312 КБ	Средний
	0640	jucheck.exe		9 892 КБ		9 912 КБ	3 672 КБ	Средний
	12E0	ICQ.exe		31 632 КБ		72 416 КБ	61 780 КБ	Средний
	0CB4	httpd.exe		11 200 КБ		11 200 КБ	9 912 КБ	Средний
	08F4	httpd.exe		9 764 КБ		9 764 КБ	6 896 КБ	Средний
	02DC	GammaTray.exe		6 752 КБ		6 752 КБ	2 524 КБ	Средний
	122C	FMPicensingService.exe		2 680 КБ		2 952 КБ	824 КБ	Средний
	03D0	explorer.exe		11 968 КБ		44 880 КБ	27 260 КБ	Средний
	01F0	dsmon.exe		12 196 КБ		12 392 КБ	6 512 КБ	Средний
	05E0	CTSjyVol.exe		9 120 КБ		9 904 КБ	4 736 КБ	Средний
	0A00	CTSVCDA.EXE		1 452 КБ		1 452 КБ	508 КБ	Средний
	0690	CTHELPER.EXE		10 632 КБ		10 644 КБ	5 840 КБ	Средний
	07A4	ctfmon.exe		7 264 КБ		7 264 КБ	2 684 КБ	Средний
	05E8	CTDVIDDET.exe		5 232 КБ		5 236 КБ	1 824 КБ	Средний
	03E0	csrss.exe		6 480 КБ		7 776 КБ	1 752 КБ	Высокий
	0978	avp.exe		7 564 КБ		73 620 КБ	50 384 КБ	Средний
	06E4	avp.exe		3 132 КБ		12 620 КБ	7 696 КБ	Средний
	0164	atitray.exe		6 680 КБ		8 768 КБ	6 508 КБ	Средний

Процессов: 66    Загрузка ЦП: 4.7%    Выделение памяти: 1878.78 МБ

# Програмне забезпечення PROWiSe Manager



The screenshot displays the PROWiSe Manager application window. The title bar reads "PROWiSe Manager". The menu bar includes "Файл", "Вид", "Процесс", "Завершение работы", and "Помощь". The toolbar contains icons for "Процессы", "Окна", "Службы", "Драйверы", "Автозагрузка", and "Быстродействие".

The main area shows a table of running processes with the following columns: "Процесс", "ID", "Описание", "ЦП", "Пользователь", "Потоки", "Вирт.п.", and "Рабочая ...".

Процесс	ID	Описание	ЦП	Пользователь	Потоки	Вирт.п.	Рабочая ...
Бездействие сис...	0	-- не удалось открыть процесс ==	99	SYSTEM	2	0 K	16 K
Interrupts	n/o	Hardware Interrupts	n/o	n/o	0	0 K	0 K
DPCs	n/o	Deferred Procedure Calls	n/o	n/o	0	0 K	0 K
System	4	-- не удалось прочитать память проц...		SYSTEM	129	1 876 K	244 K
smss.exe	936	Диспетчер сеанса Windows NT		SYSTEM	3	3 800 K	412 K
csrss.exe	992	Client Server Runtime Process		SYSTEM	15	55 468 K	6 268 K
winlogon.exe	1020	Программа входа в систему Windows NT		SYSTEM	26	58 416 K	1 132 K
services.exe	1064	Приложение служб и контроллеров		SYSTEM	15	22 620 K	3 820 K
lsass.exe	1076	LSA Shell (Export Version)		SYSTEM	20	43 168 K	1 008 K
ati2evxx.exe	1268	ATI External Event Utility EXE Module		SYSTEM	4	23 352 K	3 152 K
svchost.exe	1284	Generic Host Process for Win32 Services		SYSTEM	18	63 128 K	5 304 K
svchost.exe	1356	Generic Host Process for Win32 Services		NETWORK SERVICE	10	39 672 K	4 888 K
svchost.exe	1728	Generic Host Process for Win32 Services		SYSTEM	84	168 292 K	32 640 K
svchost.exe	1784	Generic Host Process for Win32 Services		NETWORK SERVICE	6	33 044 K	4 024 K
ati2evxx.exe	2024	ATI External Event Utility EXE Module		SYSTEM	6	28 448 K	3 368 K
svchost.exe	368	Generic Host Process for Win32 Services		LOCAL SERVICE	17	44 500 K	8 244 K
spoolsv.exe	592	Spooler Sub-System App		SYSTEM	11	45 988 K	5 924 K
wbload.exe	668	WindowBlinds		Алексей	1	34 140 K	2 116 K
explorer.exe	976	Проводник	2	Алексей	17	143 560 K	6 864 K
SMax4PNP.exe	1484	SMax4PNP MFC Application		Алексей	5	44 088 K	6 204 K
CTSysVol.exe	1504	CTSysVol.exe		Алексей	2	49 060 K	9 120 K
CTDVDDet.exe	1512	CTDVDDet.exe		Алексей	1	35 196 K	5 232 K
Jusched.exe	1556	n/o		Алексей	1	32 512 K	4 252 K
SMSTray.exe	1568	SMSTray.exe		Алексей	4	69 860 K	13 256 K
Jucheck.exe	1600	UpdateChecker Module		Алексей	4	59 328 K	9 892 K
LvAgent.exe	1624	Lingvo Launcher		Алексей	1	31 532 K	4 016 K
point32.exe	1656	Point32.exe		Алексей	4	45 400 K	6 040 K
CTHELPER.EXE	1680	CHelper Application		Алексей	5	53 500 K	10 632 K
Acrotray.exe	1880	AcroTray		Алексей	3	58 792 K	12 464 K
TrueImageMonitor...	1900	TrueImage		Алексей	4	41 864 K	7 084 K
schedhlp.exe	1908	Acronis Scheduler Helper		Алексей	1	37 428 K	6 612 K
avp.exe	1764	Kaspersky Anti-Virus		Алексей	0	101 392 K	3 188 K
ctfmon.exe	1956	CTF Loader		Алексей	1	39 440 K	7 264 K
atitray.exe	356	ATI Tray Tools		Алексей	3	60 772 K	6 688 K
daemon.exe	496	DAEMON Tools main application		Алексей	3	56 328 K	12 196 K
LogitechDesktopM...	644	Logitech Desktop Messenger		Алексей	9	76 620 K	1 556 K
GammaTray.exe	732	GammaTray MFC ????		Алексей	1	38 104 K	6 752 K
Launchy.exe	760	Launchy		Алексей	2	54 280 K	10 916 K
SetPoint.exe	772	Logitech SetPoint Event Manager		Алексей	2	53 216 K	12 120 K
NetworkLicenseSe...	1228	ABBYY network license server		SYSTEM	12	41 916 K	6 700 K
KHALMNP.R.EXE	2000	Logitech KHAL Main Process		Алексей	15	54 372 K	7 708 K
schedul2.exe	2244	Acronis Scheduler 2		SYSTEM	4	19 536 K	1 900 K
httpd.exe	2292	Apache HTTP Server		SYSTEM	3	38 464 K	9 764 K
aspnet_state.exe	2336	Microsoft ASP.NET State Server		NETWORK SERVICE	4	26 772 K	3 532 K
AdsiScSrv.exe	2372	System Level Service Utility		SYSTEM	5	15 728 K	1 332 K
avp.exe	2424	Kaspersky Anti-Virus		SYSTEM	0	175 680 K	17 148 K
mDNSResponder....	2496	Bonjour Service		SYSTEM	5	26 112 K	3 728 K
CTSVCCDA.EXE	2560	Creative Service for CD-ROM Access		SYSTEM	2	16 720 K	1 452 K
mdm.exe	2860	Machine Debug Manager		SYSTEM	4	27 580 K	3 304 K

At the bottom of the window, the status bar shows: "Процессы: 67", "Загрузка ЦП: 1%", and "05:13:08".

# Програмне забезпечення

## PrcInfo

Processes: 68 - Acrotray.exe - PrcInfo 4.28

File Threads Modules View Tools Help

Name	Full Path	ID	Parent ID	Type	Base priority	Number of Threads	Number of Windows	Creation time	Read Operations	Write Operations
[System Process]	[System Process]	0	0	32-bit	1943618225 (Normal)	2	0	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP
Acrotray.exe	Acrotray.exe	1880	976	32-bit	32 (Normal)	3	2	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP
AdskScSrv.exe	AdskScSrv.exe	2372	1064	32-bit	1943618225 (Normal)	5	0	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP
alo.exe	alo.exe	5328	1064	16-bit	1943618225 (Normal)	5	0	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP	Only for WindowsME 2000 XP

ID	Thread Priority (Delta)	Creation time
1888	8 (Normal)	Only for WindowsME 2000 XP
4792	8 (Normal)	Only for WindowsME 2000 XP
6056	8 (Normal)	Only for WindowsME 2000 XP

Name	Full Path	ID	Globale Usage Count	Size (in bytes)	Base Address
Acrotray.exe	D:\Programs\Acrobat 8.0\Acrobat\Acrotray.exe	1	65535	638 976	4 194 304
adobe_epic.dll	D:\Programs\Acrobat 8.0\Acrobat\adobe_epic.dll	1	4	237 568	14 745 600
adobe_pcd.dll	D:\Programs\Acrobat 8.0\Acrobat\adobe_pcd.dll	1	48	221 184	18 284 544
adobe_personalization.dll	D:\Programs\Acrobat 8.0\Acrobat\adobe_personalization.dll	1	4	368 640	14 286 848
ADVAPI32.dll	C:\WINDOWS\system32\ADVAPI32.dll	1	65535	704 512	2 010 906 624
appHelp.dll	C:\WINDOWS\system32\appHelp.dll	1	2	139 264	2 008 219 648
asneui.dll	D:\Programs\Acrobat 8.0\Acrobat\asneui.dll	1	42	131 072	268 435 456
CLBCATQ.DLL	C:\WINDOWS\system32\CLBCATQ.DLL	1	6	520 192	1 996 226 560
comctl32.dll	C:\WINDOWS\System32\comctl32.dll	1	3	1 060 864	2 000 420 864
COMCTL32.dll	C:\WINDOWS\system32\COMCTL32.dll	1	65535	630 784	1 566 244 864
comdlg32.dll	C:\WINDOWS\system32\comdlg32.dll	1	65535	299 008	1 983 381 504
COMRes.dll	C:\WINDOWS\system32\COMRes.dll	1	6	815 104	1 996 750 848
CRYPT32.dll	C:\WINDOWS\system32\CRYPT32.dll	1	1	614 400	2 007 433 216
davclnt.dll	C:\WINDOWS\System32\davclnt.dll	1	1	40 960	1 978 925 056
DNSAPI.dll	C:\WINDOWS\system32\DNSAPI.dll	1	2	159 744	1 995 505 664
drprov.dll	C:\WINDOWS\System32\drprov.dll	1	1	28 672	1 978 859 520
FNP_Act_Installer.dll	D:\Programs\Acrobat 8.0\Acrobat\FNP_Act_Installer.dll	1	2	950 272	1 725 956 096
GDI32.dll	C:\WINDOWS\system32\GDI32.dll	1	65535	299 008	2 012 282 880
hnetcfg.dll	C:\WINDOWS\system32\hnetcfg.dll	1	1	360 448	1 770 717 184
IadHide5.dll	C:\DOCLUME~1\07C4~1\LOCALS~1\Temp\IadHide5.dll	1	1	24 576	18 612 224
icmp.dll	C:\WINDOWS\system32\icmp.dll	1	2	16 384	1 948 581 888
IMAGEHLP.dll	C:\WINDOWS\system32\IMAGEHLP.dll	1	1	163 840	1 992 818 688
IMM32.DLL	C:\WINDOWS\system32\IMM32.DLL	1	4	118 784	1 983 250 432
iphlpapi.dll	C:\WINDOWS\system32\iphlpapi.dll	1	7	102 400	1 993 670 656
iprepair.dll	C:\Program Files\IconPacker\iprepair.dll	1	1	81 920	18 743 296
kernel32.dll	C:\WINDOWS\system32\kernel32.dll	1	65535	1 015 808	2 088 763 392
lgscroll.dll	C:\Program Files\Logitech\SetPoint\lgscroll.dll	1	1	57 344	269 484 032
mdnsNSP.dll	C:\Program Files\Bonjour\mdnsNSP.dll	1	1	102 400	369 623 040
MLANG.dll	C:\WINDOWS\system32\MLANG.dll	1	1	593 920	1 977 221 120
MPR.dll	C:\WINDOWS\system32\MPR.dll	1	1	73 728	1 907 359 744
MSASN1.dll	C:\WINDOWS\system32\MSASN1.dll	1	2	73 728	2 008 088 576
MSCTF.dll	C:\WINDOWS\system32\MSCTF.dll	1	2	311 296	1 953 366 016
msctfime.ime	C:\WINDOWS\system32\msctfime.ime	1	2	188 416	1 966 145 536
MSGINA.dll	C:\WINDOWS\system32\MSGINA.dll	1	1	1 019 904	1 972 633 600
msimg32.dll	C:\WINDOWS\system32\msimg32.dll	1	1	20 480	1 983 184 896
MSVCP60.dll	C:\WINDOWS\system32\MSVCP60.dll	1	65535	413 696	1 980 039 168
MSVCP71.dll	C:\WINDOWS\system32\MSVCP71.dll	1	1	503 808	2 084 175 872

Processes: 68 - Acrotray.exe Threads: 3 Modules: 81

NUM



# Програмне забезпечення A-squared HiJackFree

**а-squared HiJackFree 3.1**

EMSI SOFTWARE HIJACKFREE

Процессы

Имя	ID п...	Про...	Нити	Память	При...	Расположение	Ви...	Надпись
a2hijackfree.exe	2484	85.5	8	24496 K	Норма	C:\Program Files\A-squared HiJackFree\A2hijackfree.exe	Да	a-squared HiJackFree 3.1
Acrotray.exe	1880	0.0	3	12464 K	Норма	D:\Programs\Acrobat 8.0\Acrobat\Acrotray.exe	Нет	
AdslSvcSrv.exe	2372	0.0	5	1332 K	Норма	C:\Program Files\Common Files\Autodesk Shared\Service\AdslSvcSrv.exe	Нет	
alg.exe	5328	0.0	5	3728 K	Норма	C:\WINDOWS\system32\alg.exe	Нет	
aspnet_state.exe	2336	0.0	4	3532 K	Норма	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe	Нет	
ati2evxx.exe	1268	0.0	4	3152 K	Норма	C:\WINDOWS\system32\ati2evxx.exe	Нет	
ati2evxx.exe	2024	0.0	6	3368 K	Норма	C:\WINDOWS\system32\ati2evxx.exe	Нет	
atitray.exe	356	0.0	3	6704 K	Норма	C:\Program Files\ATI Tray Tools\atitray.exe	Нет	
avp.exe	1764	0.0	0	3268 K	Норма	C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 7.0\avp.exe	Нет	
avp.exe	2424	5.5	0	4212 K	Норма	C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 7.0\avp.exe	Нет	
csrss.exe	992	0.0	15	6628 K	Норма	C:\WINDOWS\system32\csrss.exe	Нет	
CTDVDDET.exe	1512	0.0	1	5232 K	Норма	C:\Program Files\Creative\SBAudio\2\DVD\Audio\CTDVDDET.EXE	Нет	
ctfmon.exe	1956	1.8	1	7264 K	Норма	C:\WINDOWS\system32\ctfmon.exe	Нет	
CTHELPER.EXE	1680	0.0	5	10632 K	Норма	C:\WINDOWS\CTHELPER.EXE	Нет	
CTSVCD.A.EXE	2560	0.0	2	1452 K	Норма	C:\WINDOWS\system32\CTsvcd.a.exe	Нет	
CTSysVol.exe	1504	0.0	2	9120 K	Норма	C:\Program Files\Creative\SBAudio\2\Surround Mixer\CTSysVol.exe	Нет	
daemon.exe	496	0.0	3	12196 K	Норма	C:\Program Files\DAEMON Tools\daemon.exe	Нет	E:\Prog\A-squared HiJackFree v.3...
explorer.exe	976	3.6	16	15224 K	Норма	C:\WINDOWS\Explorer.EXE	Да	
FNPLicensingService.exe	4652	0.0	5	2680 K	Норма	C:\Program Files\Common Files\Macrovision Shared\FLEX\Net Publisher\FNPLI...	Нет	
GammaTray.exe	732	0.0	1	6752 K	Норма	C:\Program Files\MagicTune3.6_Client_pivot\GammaTray.exe	Нет	
httpd.exe	2292	0.0	3	9764 K	Норма	F:\Apache 2.2\bin\httpd.exe	Нет	
httnfd.exe	3252	0.0	252	11200 K	Норма	F:\Apache 2.2\bin\httnfd.exe	Нет	

Процесс: a2hijackfree.exe

Описание: C:\Program Files\A-squared HiJackFree\A2hijackfree.exe

**Свойства файла:**

Имя файла: a2hijackfree.exe  
Путь файла: C:\Program Files\A-squared HiJackFree\  
Описание: a-squared HiJackFree  
Компания: Emsi Software GmbH  
Версия: 3.1.0.16  
Авторство: (C) 2003-2008 Emsi Software GmbH

**Детали процесса:**

Запущен как служба: Нет  
Автозапуск есть: Нет  
Открытые TCP-порты: -  
Открытые UDP-порты: -

**Загруженные модули:**

C:\Program Files\A-squared HiJackFree\A2hijackfree.exe  
C:\WINDOWS\system32\ntdll.dll  
C:\WINDOWS\system32\kernel32.dll

-- Закреть --

# Основні методи відображення прихованих процесів

Програмні методи знаходження прихованих процесів

User Mode

через ToolHelp API

через Native API

за списком відкритих хендлів

за допомогою прямого системного виклику

за списком відкритих за списком відкритих ними вікон

шляхом аналізу пов'язаних з ним хендлів

Kernel Mode

через ZwQuerySystemInformation

із двуз'язного списку структур EPROCESS

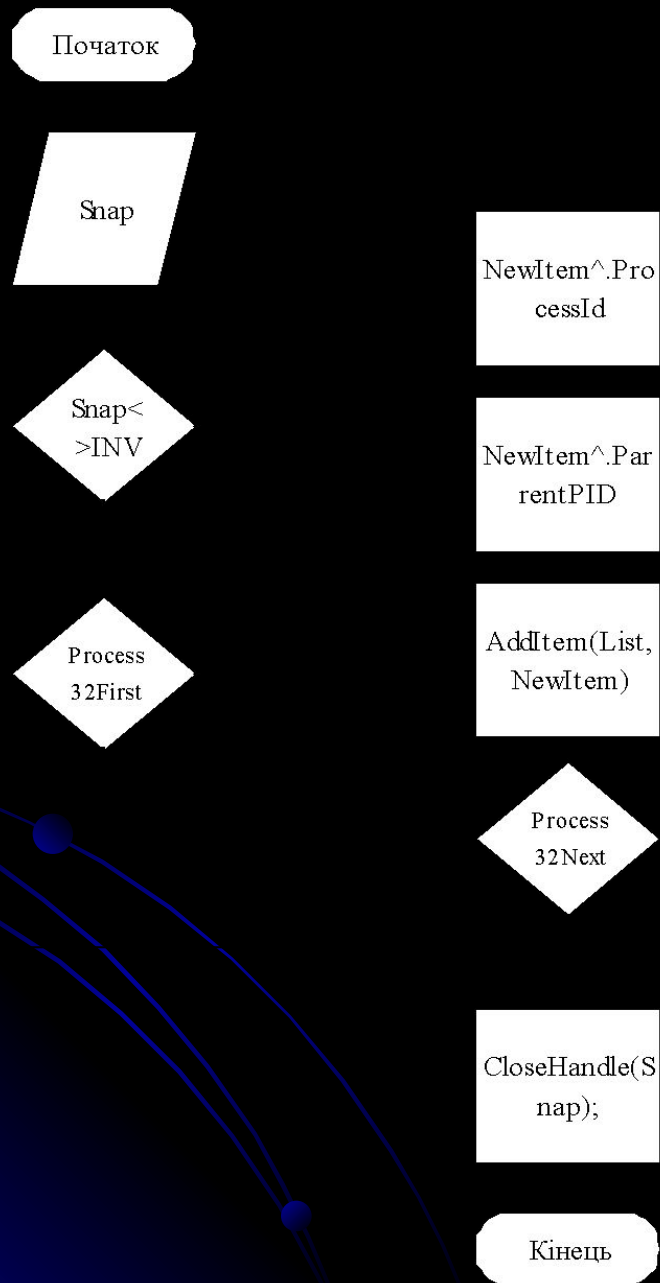
за списками потоків планувальника

перехопленням системних викликів

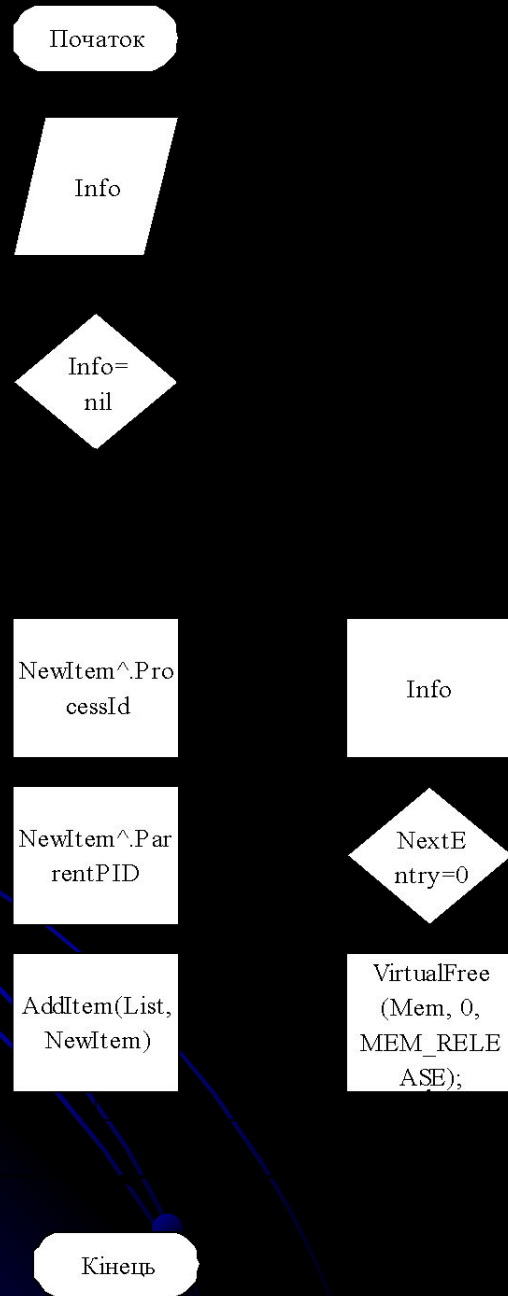
переглядом списку таблиць хендлів

шляхом сканування PspCidTable

# Схема алгоритму отримання списку процесів через ToolHelp API



# Схема алгоритму отримання списку процесів через Native API



# Вид головного вікна у полегшеному режимі сканування

The screenshot displays the Sys\_Mon application window. The main area is divided into three sections: Processes, Performance Info, and Terminal.

**Processes**

PID	CPU, %	Name	Creation Time	Running Time	Kernel Time	User Time
4		System				
620		smss.exe				
708		winlogon.exe				
752		services.exe				
764		lsass.exe				
916		svchost.exe				
1096		svchost.exe				
1592		explorer.exe				
1712		spoolsv.exe				
1828		winampa.exe				
1836		acrotray.exe				
1868		nod32kui.exe				
1884		pragma.exe				
1940		PDVDServ.exe				
1988		SMTTray.exe				
2032		StatusClient.exe				

**Performance Info**

CommitLimit □ □ 727816  
CommitPeak □ □ 86758  
CommitTotal □ □ 85411  
HandleCount □ □ 10624  
KernelNonpaged □ 7491  
KernelPaged □ □ 15424  
KernelTotal □ □ 22915  
PageSize □ □ 4096  
PhysicalAvailable 134818  
PhysicalTotal □ 261820  
ProcessCount □ 55  
SystemCache □ □ 166884  
ThreadCount □ □ 580

**Terminal**

```
$Terminal :>
01/01/1601 @ 03:00:00
148817d 6h 55m 4294967288s
0h 0m 6s
0h 0m 0s

Modules
-----
CreateToolhelp32Snapshot (of modules)
Threads
-----
THREAD ID = 0x00000008
base priority = 0
delta priority = 0
THREAD ID = 0x00000010
base priority = 13
delta priority = 0
THREAD ID = 0x00000014
base priority = 13
delta priority = 0
THREAD ID = 0x00000018
base priority = 13
delta priority = 0
THREAD ID = 0x0000001C
base priority = 13
delta priority = 0
THREAD ID = 0x00000020
base priority = 13
delta priority = 0
THREAD ID = 0x00000024
base priority = 12
delta priority = 0
THREAD ID = 0x00000028
base priority = 12
delta priority = 0
THREAD ID = 0x0000002C
base priority = 12
```

# Вид головного вікна у поглибленому режимі сканування

The screenshot displays the Sys\_Mon application window. The main area shows a list of processes with columns for PID, CPU %, Name, Creation Time, Running Time, Kernel Time, and User Time. The [System Process] is highlighted. Below the process list is a Performance Info section with various system metrics. On the right side, there is a Terminal window showing system information and thread details.

PID	CPU, %	Name	Creation Time	Running Time	Kernel Time	User Time
3392		wscntfy.exe				
3872		Generic.exe				
592		epmworker.exe				
840		cidaemon.exe				
3032		WINWORD.EXE				
308		msimn.exe				
496		WinRAR.exe				
2464		Sys_Mon.exe				
3404	0	alg.exe	06/13/2008 @ 09:55:16	0d 0h 0m 0s	0h 0m 0s	0h 0m 0s
2152	0	wdfmgr.exe	06/13/2008 @ 09:40:22	0d 0h 14m 54s	0h 0m 0s	0h 0m 0s
1224	0	svchost.exe	06/13/2008 @ 09:40:08	0d 0h 15m 8s	0h 0m 0s	0h 0m 0s
1148		svchost.exe				
996	0	svchost.exe	06/13/2008 @ 09:39:59	0d 0h 15m 17s	0h 0m 0s	0h 0m 2s
684	0	csrss.exe	06/13/2008 @ 09:39:59	0d 0h 15m 17s	0h 0m 0s	0h 0m 0s
0	0	[System Process]	06/13/2008 @ 09:39:54	0d 0h 15m 22s	0h 0m 0s	0h 0m 0s

**Performance Info**

- CommitLimit □□ 727816
- CommitPeak □□ 86758
- CommitTotal □□ 85411
- HandleCount □□ 10624
- KernelNonpaged □ 7491
- KernelPaged □□ 15424
- KernelTotal □□ 22915
- PageSize □□ 4096
- PhysicalAvailable 134818
- PhysicalTotal □ 261820
- ProcessCount □ 55
- SystemCache □□ 166884
- ThreadCount □□ 580

**\$Terminal :>**

```
01/01/1601 @ 03:00:00
148817d 6h 55m 4294967288s
0h 0m 6s
0h 0m 0s

Modules
CreateToolhelp32Snapshot (of mod
Threads
THREAD ID = 0x00000008
base priority = 0
delta priority = 0
THREAD ID = 0x00000010
base priority = 13
delta priority = 0
THREAD ID = 0x00000014
base priority = 13
delta priority = 0
THREAD ID = 0x00000018
base priority = 13
delta priority = 0
THREAD ID = 0x0000001C
base priority = 13
delta priority = 0
THREAD ID = 0x00000020
base priority = 13
delta priority = 0
THREAD ID = 0x00000024
base priority = 12
delta priority = 0
THREAD ID = 0x00000028
base priority = 12
delta priority = 0
THREAD ID = 0x0000002C
base priority = 12
```

Дякую за увагу!!!  
Зустрінемося на лекції через  
ТИЖДЕНЬ

Знайти лектора можна в аудиторії 5-214

або

за e-mail-ом: [earth@ukr.net](mailto:earth@ukr.net)

або

вКонтакте: <http://vk.com/id6416748>