



ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ

ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное
образовательное учреждение города Москвы

«Колледж малого бизнеса № 4»

(ГБПОУ КМБ № 4)

Отчёт по практической работе №1

Специальность: 09.02.07 Информационные системы и программирование

Форма обучения: очная

Студент: Межибор Ярослав Евгеньевич

Группа: ИПО-21.24

Проверил: Рыбаков Александр Сергеевич

Москва, 2025 г.

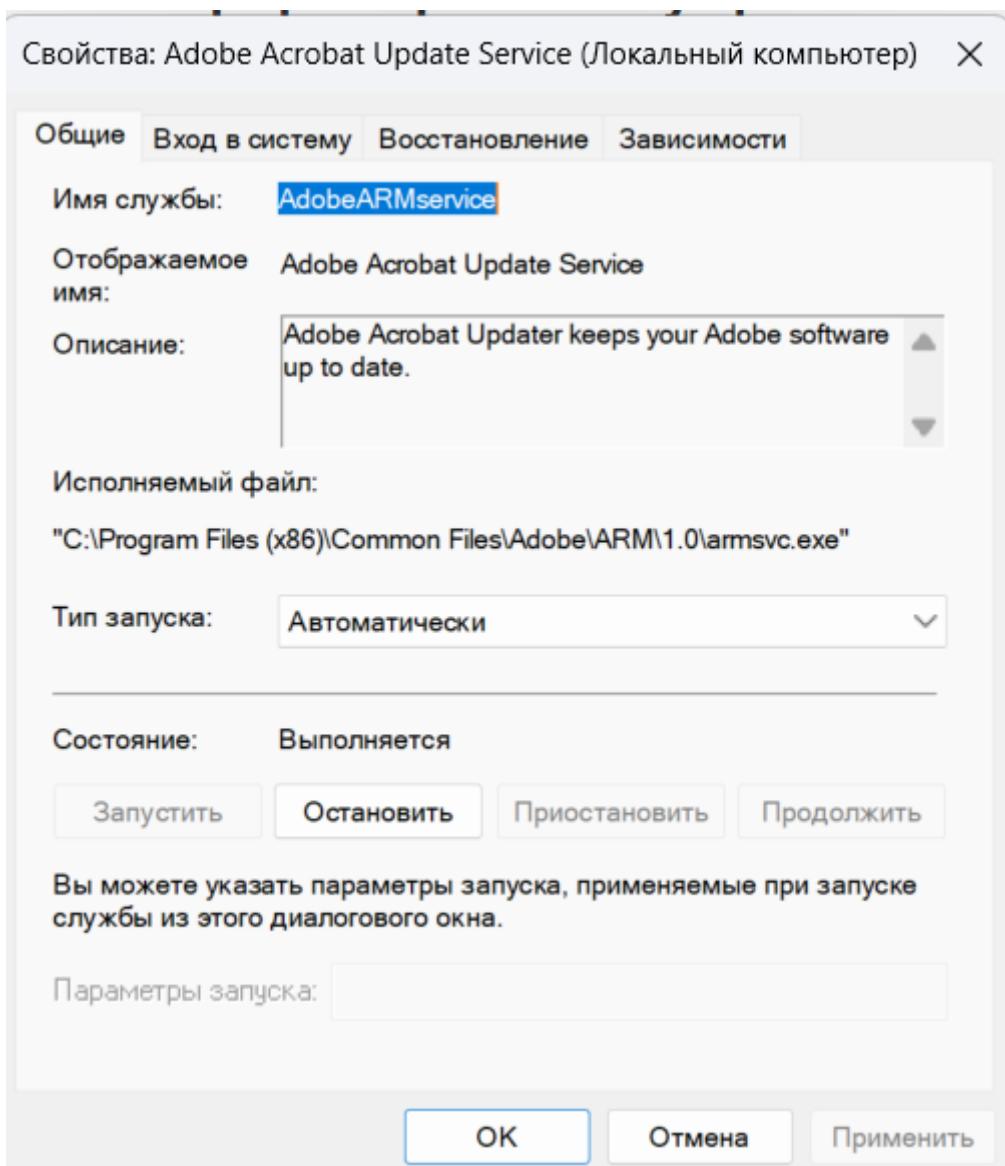


Рис. 1. Сортировка служб по состоянию после нажатия на Состояния

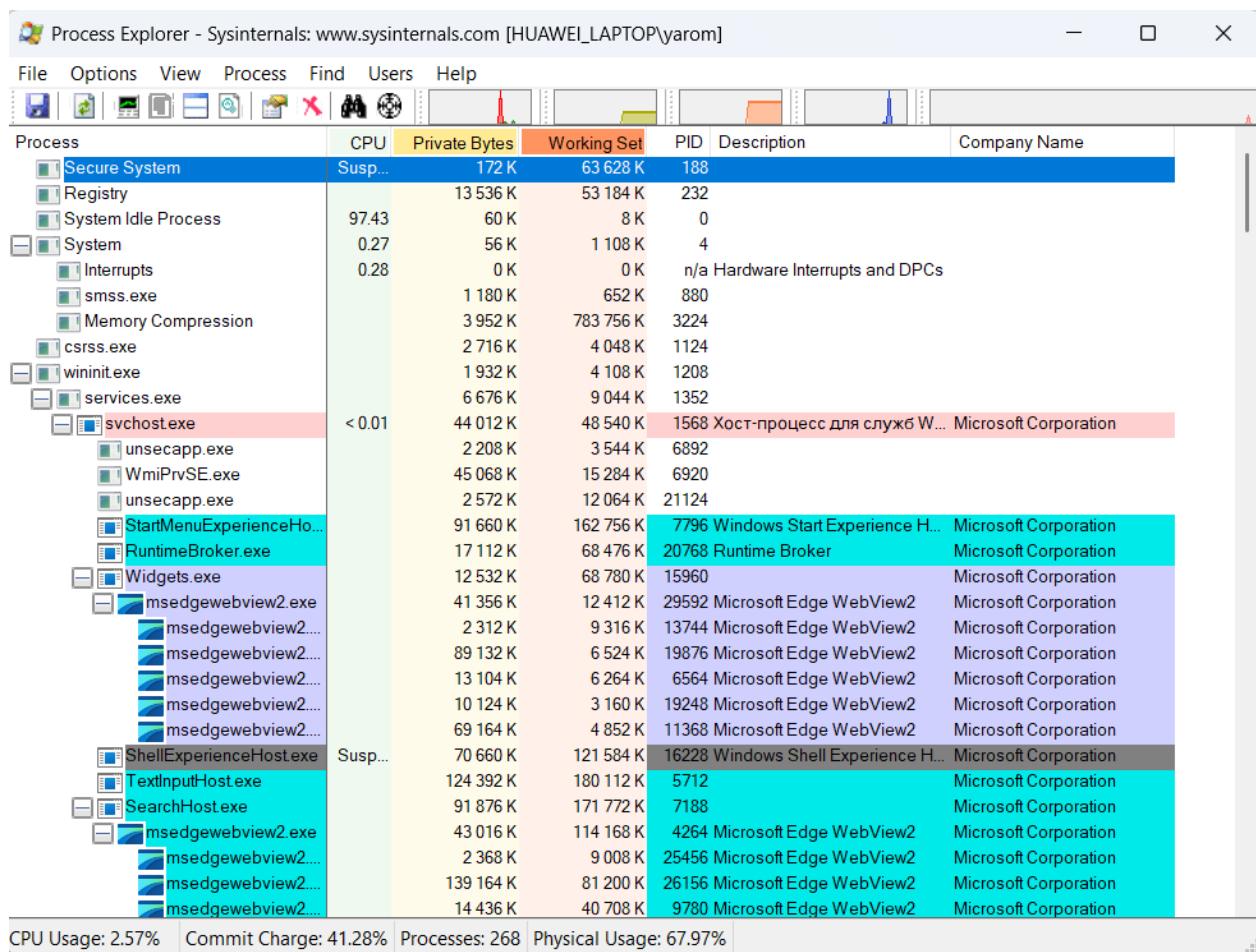


Рис. 2. Показ дерева процессов в Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

The screenshot shows the Process Explorer application window. The main pane displays a list of processes sorted by CPU usage. The columns shown are Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The top process listed is msedgewebview2.exe, which is consuming the most CPU resources.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
msedgewebview2.exe	9 840 K	20 072 K	5920	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	41 260 K	7 412 K	29592	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	2 312 K	9 272 K	13744	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	89 168 K	1 856 K	19876	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	13 560 K	2 316 K	6564	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	10 128 K	1 668 K	19248	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	64 112 K	2 100 K	11368	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	9 216 K	6 952 K	21000	Microsoft Edge WebView2	Microsoft Corporation	
msedgewebview2.exe	86 480 K	106 472 K	12632	Microsoft Edge WebView2	Microsoft Corporation	
mysqld.exe	33 968 K	3 192 K	4836		Oracle Corporation	
Ngclso.exe	13 912 K	2 552 K	4152			
NisSrv.exe	4 596 K	5 588 K	12484	Microsoft Network Realtime I...	Microsoft Corporation	
Notepad.exe	123 056 K	95 816 K	2496			
OneApp.IGCC.WinService.exe	40 276 K	13 104 K	4480	Intel® Graphics Command Ce...	Intel Corporation	
osdservice.exe	3 732 K	8 548 K	4512	osdservice.exe	Huawei Device Co., Ltd.	
procexp.exe	3 396 K	12 972 K	16400	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
Registry	13 528 K	53 348 K	232			
RuntimeBroker.exe	17 112 K	68 104 K	20768	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	2 316 K	13 272 K	26524	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	8 944 K	47 184 K	11844	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	5 160 K	34 788 K	22844	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe	2 456 K	14 388 K	18936	Runtime Broker	Microsoft Corporation	
SearchFilterHost.exe	2 016 K	12 140 K	6240			
SearchFilterHost.exe	2 024 K	12 528 K	4252			
SearchHost.exe	91 992 K	141 348 K	7188		Microsoft Corporation	
SearchProtocolHost.exe	2 736 K	19 324 K	29192			
Secure System	Susp...	172 K	63 628 K	188		
SecurityHealthService.exe		11 324 K	14 988 K	3520 Windows Security Health Ser...	Microsoft Corporation	
SecurityHealthSystray.exe		1 980 K	13 028 K	25056 Windows Security notification ...	Microsoft Corporation	
SenaryAudioApp.exe		65 484 K	67 104 K	14272 Senary Audio Application	Senary Technology Limited	

CPU Usage: 4.68% Commit Charge: 41.84% Processes: 271 Physical Usage: 67.01%

Рис. 3. Сортировка списка процессов по потреблению ресурсов

Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

The screenshot shows the Process Explorer application window. The main pane displays a list of processes sorted by Private Bytes usage. The columns shown are Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The list includes various Microsoft services like RuntimeBroker.exe, svchost.exe, msedge.exe, and Google Chrome processes. The company names listed are Microsoft Corporation, Google LLC, and Huawei Device Co., Ltd.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
RuntimeBroker.exe		5 212 K	34 800 K	22844	Runtime Broker	Microsoft Corporation
svchost.exe	< 0.01	11 480 K	34 820 K	17304	Хост-процесс для служб W...	Microsoft Corporation
svchost.exe		92 176 K	35 588 K	3628	Хост-процесс для служб W...	Microsoft Corporation
DFSSearchService.exe	< 0.01	24 764 K	37 488 K	20764		
msedge.exe	< 0.01	16 508 K	39 504 K	2648	Microsoft Edge	Microsoft Corporation
msedgewebview2.exe	< 0.01	14 352 K	39 908 K	9780	Microsoft Edge WebView2	Microsoft Corporation
svchost.exe	< 0.01	38 612 K	40 644 K	4464	Хост-процесс для служб W...	Microsoft Corporation
svchost.exe		10 156 K	42 248 K	19060	Хост-процесс для служб W...	Microsoft Corporation
ctfmon.exe		28 124 K	42 292 K	28012		
chrome.exe		67 632 K	42 320 K	9824	Google Chrome	Google LLC
msedge.exe		69 468 K	43 144 K	21352	Microsoft Edge	Microsoft Corporation
chrome.exe		17 108 K	45 256 K	27012	Google Chrome	Google LLC
svchost.exe		44 224 K	46 580 K	1568	Хост-процесс для служб W...	Microsoft Corporation
RuntimeBroker.exe		9 012 K	47 204 K	11844	Runtime Broker	Microsoft Corporation
svchost.exe		11 528 K	47 728 K	9008	Хост-процесс для служб W...	Microsoft Corporation
ApplicationFrameHost.exe		64 872 K	49 092 K	16392	Application Frame Host	Microsoft Corporation
HiviewService.exe	< 0.01	22 164 K	51 204 K	9456		
ShellHost.exe		43 472 K	51 952 K	17268	ShellHost	Microsoft Corporation
chrome.exe		19 152 K	51 960 K	22368	Google Chrome	Google LLC
chrome.exe		28 584 K	52 192 K	18292	Google Chrome	Google LLC
Registry		13 596 K	53 360 K	232		
HwMdcUI.exe	< 0.01	146 852 K	53 912 K	14912	HwMdcUI	Huawei Device Co., Ltd.
sihost.exe		10 172 K	53 912 K	340	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		49 520 K	54 816 K	4412	Хост-процесс для служб W...	Microsoft Corporation
DataExchangeHost.exe		15 020 K	55 080 K	11448	Узел обмена данными	Microsoft Corporation
chrome.exe		55 264 K	55 352 K	17608	Google Chrome	Google LLC
chrome.exe		27 660 K	56 348 K	4452	Google Chrome	Google LLC
node.exe		33 224 K	62 392 K	28324	Node.js JavaScript Runtime	Node.js
Secure System	Susp...	172 K	63 628 K	188		
procexp64.exe		0.81	32 540 K	64 608 K	27892 Sysinternals Process Explorer	Sysinternals - www.sysinter...

CPU Usage: 2.96% Commit Charge: 41.83% Processes: 270 Physical Usage: 67.45%

Рис. 4. Сортировка списка процессов по потреблению ресурсов оперативной памяти

Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

The screenshot shows the Process Explorer application window. The title bar reads "Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]". The menu bar includes File, Options, View, Process, Find, Users, and Help. Below the menu is a toolbar with various icons. The main area is a grid table with the following columns: Process, Working Set, PID, Description, Company Name, I/O Read Bytes, and I/O Write Bytes. The table lists numerous processes, including system services like Intel PIE Service, Intel Audio Service, and various Microsoft and Intel drivers. The rows are color-coded in shades of pink, blue, and grey. The "Working Set" column shows memory usage in kilobytes (K). The "I/O Read Bytes" column is highlighted in blue, indicating it is the sorting key. The "Secure System" process at the bottom is highlighted in blue.

Process	Working Set	PID	Description	Company Name	I/O Read Bytes	I/O Write Bytes
Intel_PIE_Service.exe	2 844 K	10020	SHA1:0xefecbf60	Intel Corporation		
IntelAudioService.exe	7 004 K	4504	IntelAudioService	Intel		
IntelCpHDPSvc.exe	1 956 K	2264	Intel HD Graphics Drivers for ...	Intel Corporation		
Interrupts	0 K	n/a	Hardware Interrupts and DPCs			
ipf_uf.exe	4 356 K	5416	Intel(R) Innovation Platform Fr...	Intel Corporation		
ipfsvc.exe	2 284 K	5332	Intel(R) Innovation Platform Fr...	Intel Corporation		
jhi_service.exe	1 392 K	6272	Intel(R) Dynamic Application ...	Intel Corporation		
LCD_Service.exe	13 152 K	4616	LCD_Service	Huawei Device Co., Ltd.		
Lsalso.exe	1 696 K	1364				
Lsass.exe	23 456 K	1380	Local Security Authority Proc...	Microsoft Corporation		
MateBookService.exe	17 424 K	4648	MBAMainService	Huawei Device Co., Ltd.		
MBAMessageCenter.exe	65 460 K	11752				
Memory Compression	917 940 K	3224				
MpDefenderCoreService.exe	15 352 K	4736	Antimalware Core Service	Microsoft Corporation		
MsMpEng.exe	236 832 K	4780	Antimalware Service Execut...	Microsoft Corporation		
mysqld.exe	3 168 K	4836		Oracle Corporation		
mysqld.exe	3 684 K	5428				
NgcIso.exe	2 228 K	4152				
NisSrv.exe	5 684 K	12484	Microsoft Network Realtime I...	Microsoft Corporation		
OfficeClickToRun.exe	22 460 K	4492	Microsoft Office Click-to-Run (...	Microsoft Corporation		
OneApp.IGCC.WinService.exe	13 024 K	4480	Intel® Graphics Command Ce...	Intel Corporation		
osdservice.exe	8 140 K	4512	osdservice.exe	Huawei Device Co., Ltd.		
Registry	53 876 K	232				
SearchFilterHost.exe	12 288 K	6240				
SearchFilterHost.exe	12 868 K	4252				
SearchIndexer.exe	32 104 K	12772	Индексатор службы Micros...	Microsoft Corporation		
SearchProtocolHost.exe	19 316 K	29192				
Secure System	63 628 K	188				
SecurityHealthService.exe	14 880 K	3520	Windows Security Health Ser...	Microsoft Corporation		
SenaryAudioApp.Svc.exe						

CPU Usage: 6.38% | Commit Charge: 42.12% | Processes: 271 | Physical Usage: 66.08%

Рис. 5. Сортировка списка процессов по объёму прочитанных данных

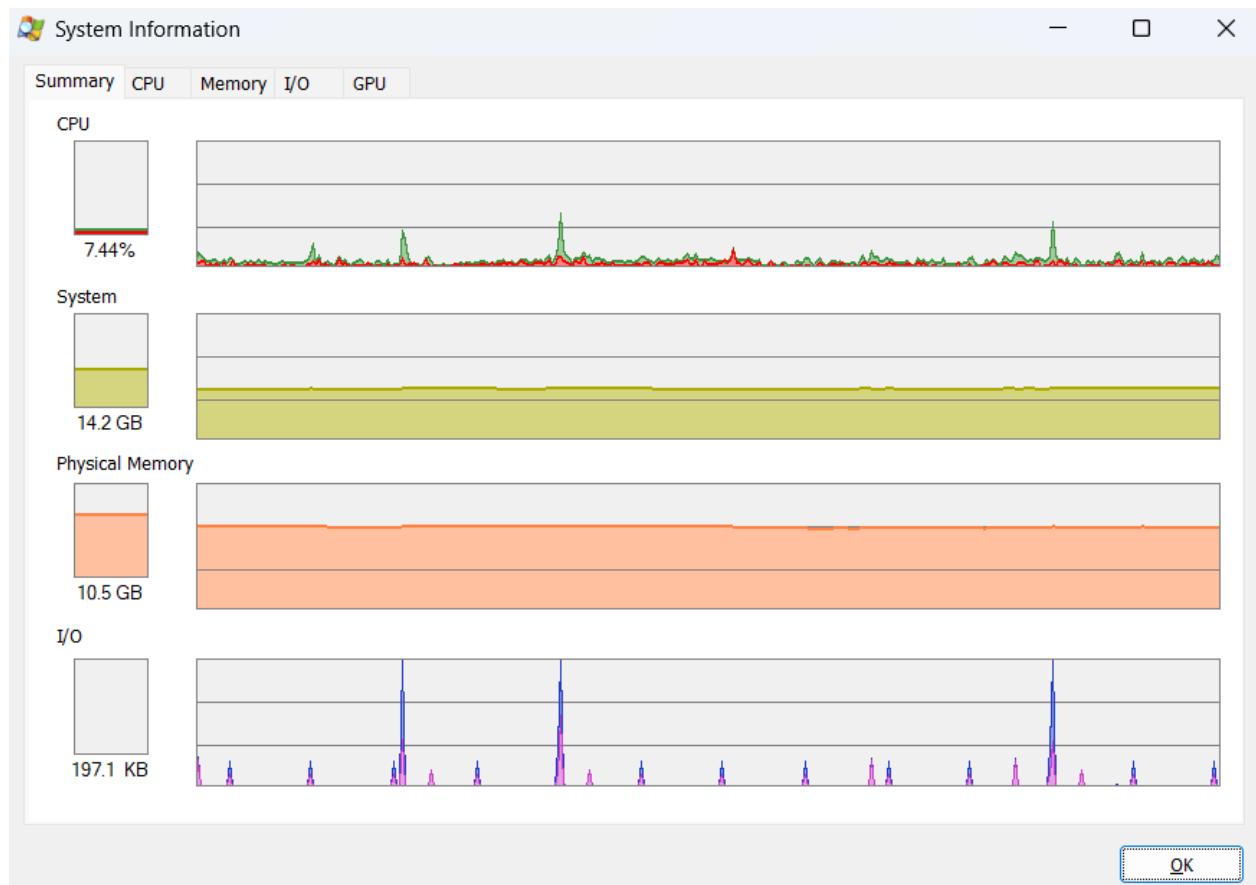
Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

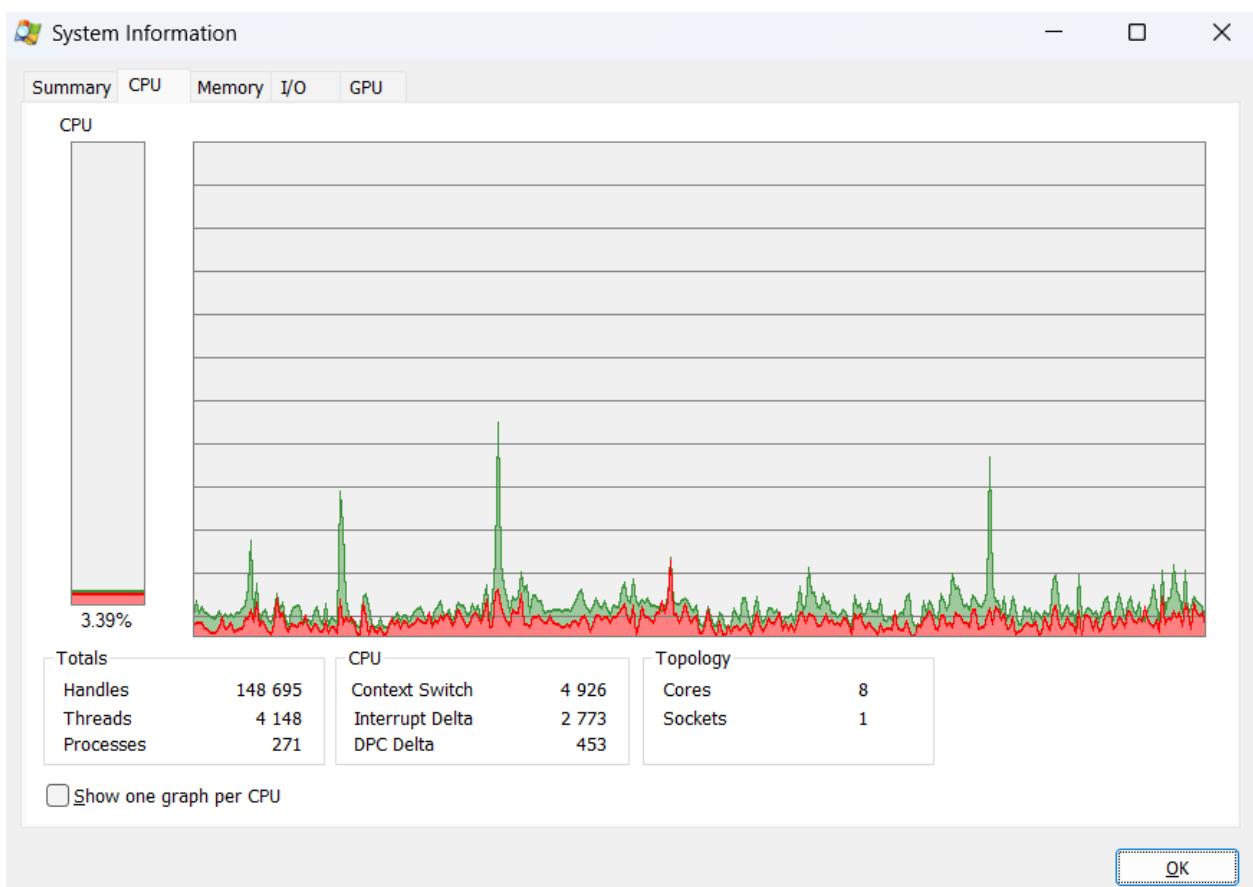
The screenshot shows the Process Explorer application window. The title bar reads "Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]". The menu bar includes File, Options, View, Process, Find, Users, and Help. Below the menu is a toolbar with various icons. The main area is a grid table with columns: Process, Working Set, PID, Description, Company Name, I/O Read Bytes, and I/O Write Bytes. The table lists numerous processes, with "LockApp.exe" highlighted in grey. The rows are color-coded in a repeating pattern of light red, light blue, and light green. At the bottom of the table, there is a status bar with CPU Usage: 4.06%, Commit Charge: 41.95%, Processes: 268, and Physical Usage: 66.22%.

Process	Working Set	PID	Description	Company Name	I/O Read Bytes	I/O Write Bytes
ipfsvc.exe	2 284 K	5332	Intel(R) Innovation Platform Fr...	Intel Corporation		
jh!_Service.exe	1 392 K	6272	Intel(R) Dynamic Application ...	Intel Corporation		
LCD_Service.exe	13 152 K	4616	LCD_Service	Huawei Device Co., Ltd.		
LockApp.exe	75 004 K	5704	LockApp.exe	Microsoft Corporation	48.5 KB	
Lsalso.exe	1 696 K	1364				
lsass.exe	23 436 K	1380	Local Security Authority Proc...	Microsoft Corporation		
MateBookService.exe	17 508 K	4648	MBAMainService	Huawei Device Co., Ltd.		
MBAMessageCenter.exe	65 476 K	11752				
Memory Compression	916 676 K	3224				
MoNotificationUx.exe	13 472 K	9204	Хост-процесс для уведомл...	Корпорация Майкрософ...	11.2 KB	
MpDefenderCoreService.exe	15 360 K	4736	Antimalware Core Service	Microsoft Corporation		
MsMpEng.exe	223 848 K	4780	Antimalware Service Execut...	Microsoft Corporation		
mysqld.exe	3 168 K	4836		Oracle Corporation		
mysqld.exe	3 684 K	5428				
Ngclso.exe	2 228 K	4152				
NisSrv.exe	5 672 K	12484	Microsoft Network Realtime I...	Microsoft Corporation		
OfficeClickToRun.exe	22 508 K	4492	Microsoft Office Click-to-Run (...)	Microsoft Corporation		
OneApp.IGCC.WinService.exe	13 060 K	4480	Intel® Graphics Command Ce...	Intel Corporation		
osdservice.exe	8 140 K	4512	osdservice.exe	Huawei Device Co., Ltd.		
Registry	53 212 K	232				
RuntimeBroker.exe	13 216 K	26524	Runtime Broker	Microsoft Corporation	6.5 KB	
RuntimeBroker.exe	34 736 K	22844	Runtime Broker	Microsoft Corporation	56.1 KB	
RuntimeBroker.exe	14 372 K	18936	Runtime Broker	Microsoft Corporation	6.9 KB	
SearchFilterHost.exe	12 128 K	6240				
SearchFilterHost.exe	12 812 K	4252				
SearchIndexer.exe	32 192 K	12772	Индексатор службы Micros...	Microsoft Corporation		
SearchProtocolHost.exe	18 008 K	29192				
Secure System	63 628 K	188				
SecurityHealthService.exe	14 896 K	3520	Windows Security Health Ser...	Microsoft Corporation		
SecurityHealthStray.exe						

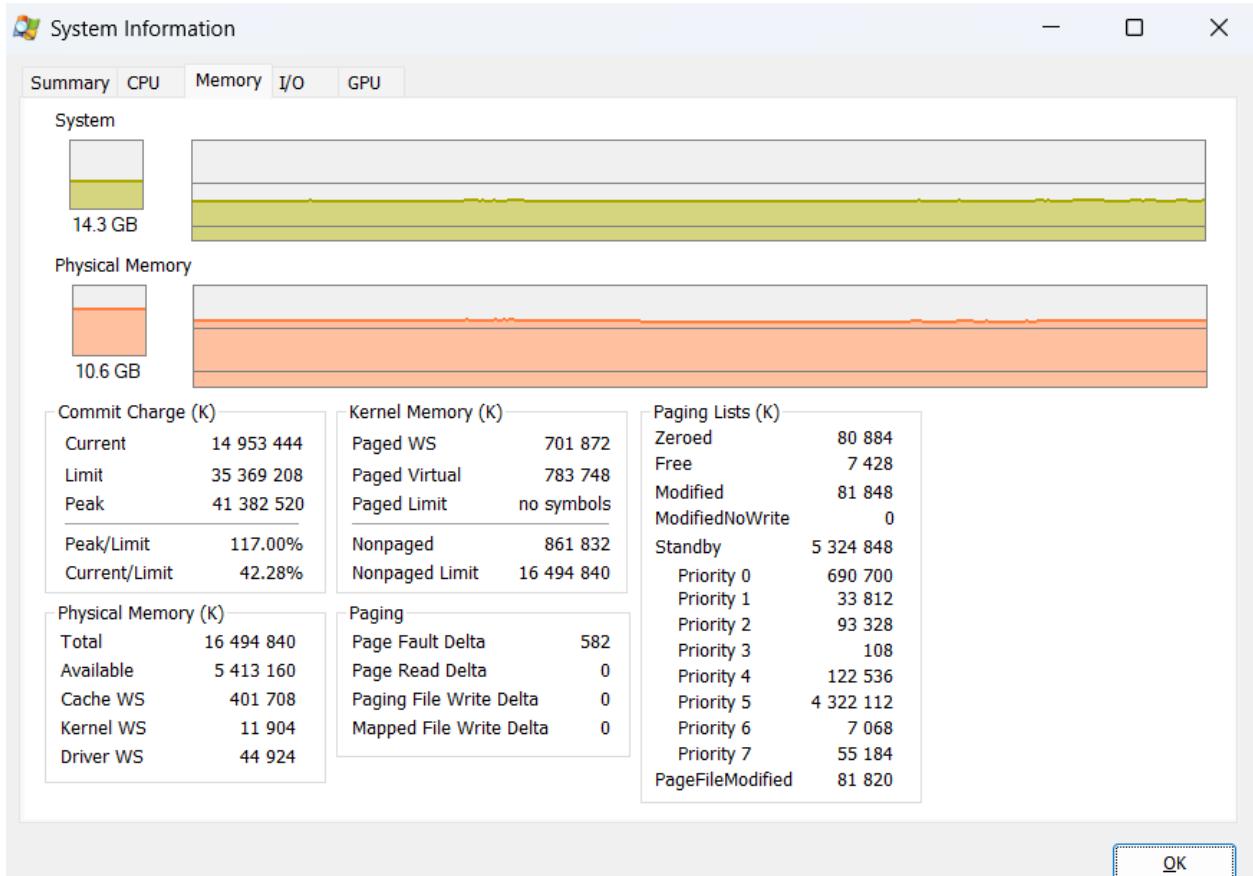
CPU Usage: 4.06% | Commit Charge: 41.95% | Processes: 268 | Physical Usage: 66.22%

Рис. 6. Сортировка списка процессов по объёму записанных данных





Puc. 7



Puc. 8

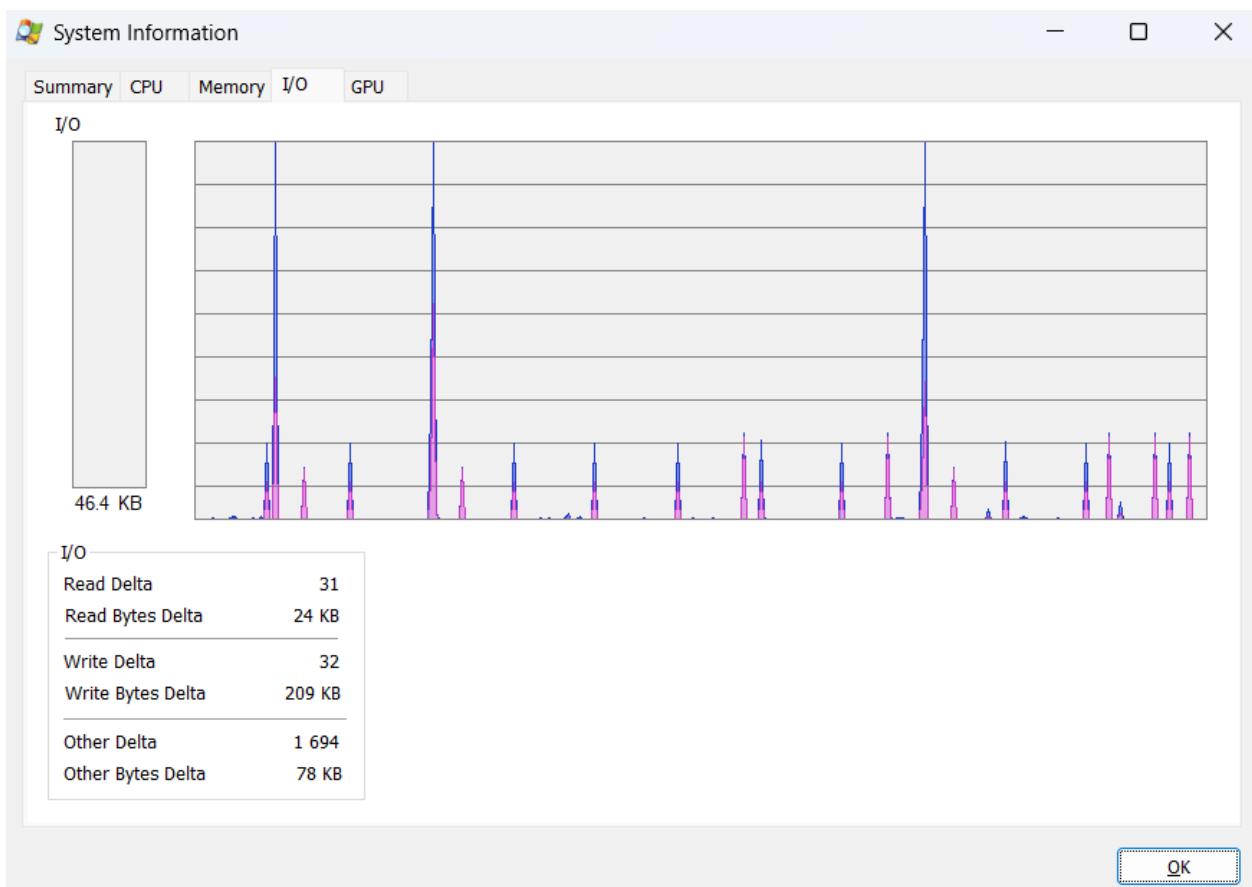


Рис. 9

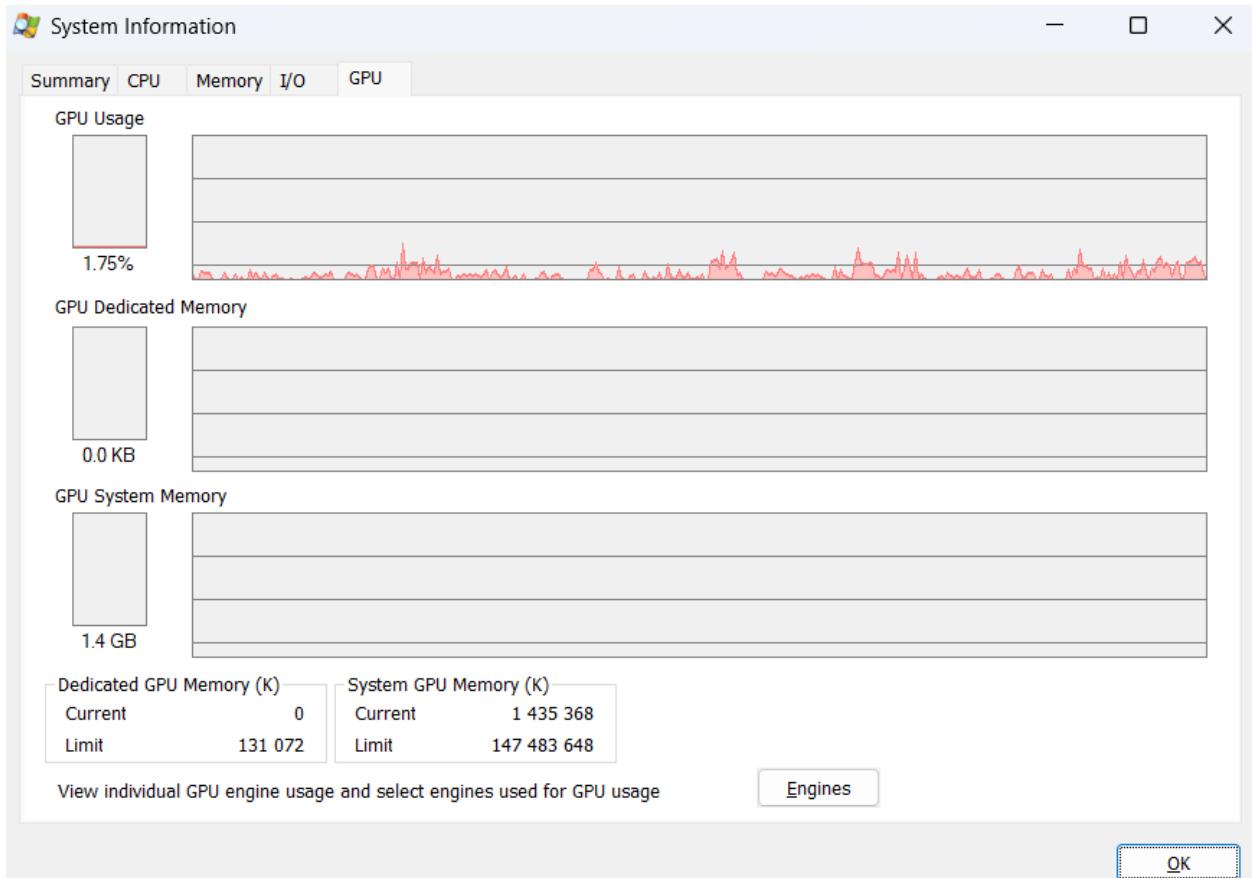


Рис. 10. Количество ядер процессора – 8, объём оперативной памяти компьютера – 10.4

Суммарный процент использования ресурсов процессора – 5%

Суммарный процент использования ресурсов оперативной памяти и файла подкачки – 42%

Общее количество процессов – 262

Суммарный процент использования ресурсов оперативной памяти – 67%

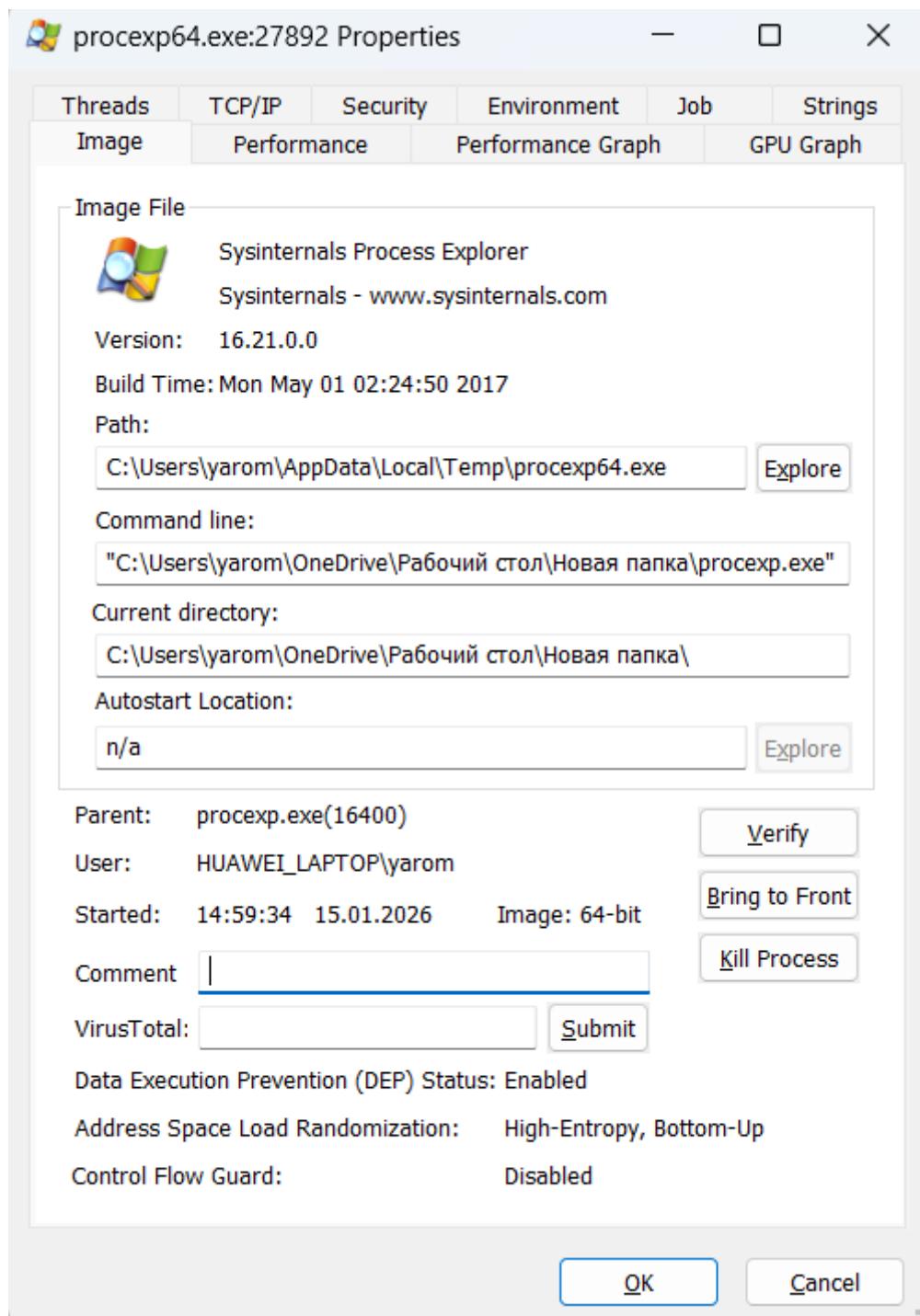


Рис. 11. Экранный снимок процесса

Путь к исполняемому файлу процесса - C:\Users\yarom\AppData\Local\Temp\procexp64.exe

Имя запустившего процесс пользователя - HUAWEI_LAPTOP\yarom

Время запуска процесса - 14:59:34

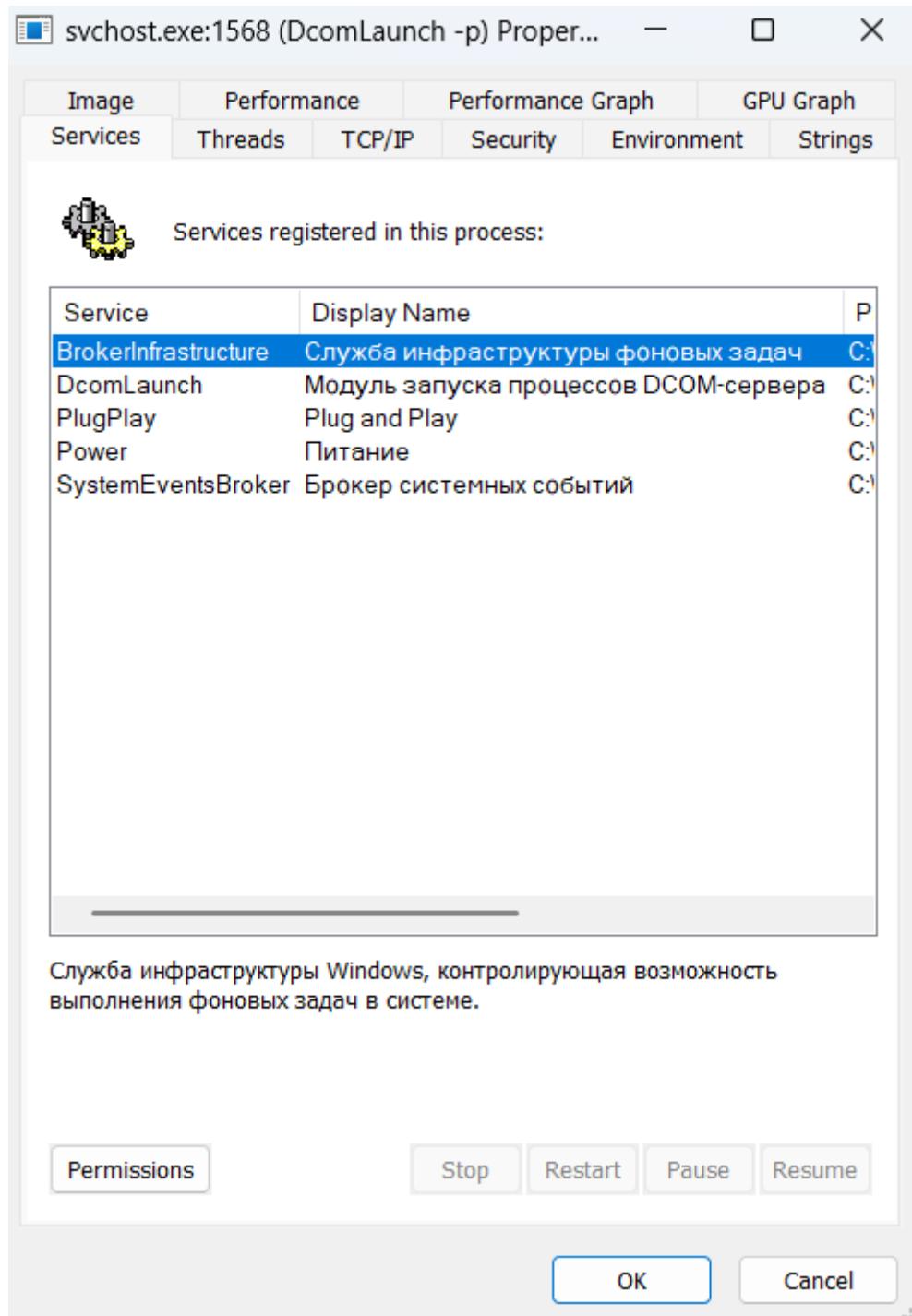


Рис. 12. Вкладка Services в процессе с наибольшим потреблением памяти svhost

Process Explorer Search

Handle or DLL substring: kernel32.dll

Search Cancel

Process	PID	Type	Name
sihost.exe	340	DLL	C:\Windows\System32\kernel32.dll
UserOOBEB...	896	DLL	C:\Windows\System32\kernel32.dll
chrome.exe	1040	DLL	C:\Windows\System32\kernel32.dll
msedge.exe	1884	DLL	C:\Windows\System32\kernel32.dll
Notepad.exe	2496	DLL	C:\Windows\System32\kernel32.dll
msedge.exe	2648	DLL	C:\Windows\System32\kernel32.dll
WidgetServi...	3176	DLL	C:\Windows\System32\kernel32.dll
msedge.exe	3624	DLL	C:\Program Files\WindowsApps\Microsoft.LanguageE...

114 matching items.

Рис. 13. Список процессов, использующих конкретную разделяемую библиотеку

Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

File Options View Process Find DLL Users Help

Process	Working Set	PID	Description	Company Name	I/O Read Bytes	I/O Write Byt
msedgewebview2.exe	91 544 K	12632	Microsoft Edge WebView2	Microsoft Corporation	17.7 MB	14.3
msedge.exe	152 604 K	3624	Microsoft Edge	Microsoft Corporation	32.1 MB	15.4
chrome.exe	132 672 K	13772	Google Chrome	Google LLC	489.1 MB	22.9
taskhostw.exe	23 656 K	16144	Хост-процесс для задач W...	Microsoft Corporation	5.3 MB	23.1
msedgewebview2.exe	110 424 K	4264	Microsoft Edge WebView2	Microsoft Corporation	57.5 MB	49.5
chrome.exe	156 964 K	16932	Google Chrome	Google LLC	12.0 MB	54.8
Telegram.exe	229 240 K	20496	Telegram Desktop	Telegram FZ-LLC	87.7 MB	56.6
explorer.exe	415 068 K	18408	Проводник	Microsoft Corporation	128.7 MB	59.1
chrome.exe	49 356 K	27812	Google Chrome	Google LLC	21.7 MB	322.2
chrome.exe	67 820 K	5780	Google Chrome	Google LLC	62.3 MB	888.9
svchost.exe	42 604 K	19060	Хост-процесс для служб W...	Microsoft Corporation	37.9 MB	922.3
chrome.exe	258 848 K	28136	Google Chrome	Google LLC	6.1 GB	5.9

Name	Description	Company Name	Path
(3DA71D5A-20CC-4...			C:\Users\yarom\AppData\Local\Microsoft\Windows\Caches\...
(6AF0698E-D558-4F...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D5...
(AFBF9F1A-8EE8-4...			C:\Users\yarom\AppData\Local\Microsoft\Windows\Caches\...
(DDF571F2-BE98-42...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE...
~FontCache-FontFa...			~FontCache-FontFace.dat \ LocalService\{AppData\Local\...
~FontCache-S-1-5-2...			C:\Windows\ServiceProfiles\LocalService\{AppData\Local\...
1307064516.pri			C:\Windows\rescache\merged\{3865704089\}1307064516.pri
2022808142.pri			C:\Windows\rescache\merged\{2504751473\}2022808142.pri
3690080027.pri			C:\Windows\rescache\merged\{637870051\}3690080027.pri
AboveLockAppHost..	AboveLockAppHost	Microsoft Corporation	C:\Windows\System32\AboveLockAppHost.dll
ActionCenter.dll	Центр безопасности и обслуги...	Microsoft Corporation	C:\Windows\System32\ActionCenter.dll
ActionCenter.dll.mui	Центр безопасности и обслуги...	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.LanguageExperie...
ActivationClient.dll	Activation Client	Microsoft Corporation	C:\Windows\System32\ActivationClient.dll
actxprxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation	C:\Windows\System32\actxprxy.dll
AdaptiveCards.OBJ...			C:\Windows\SystemApps\MicrosoftWindows.Client.Core_cw...
AdaptiveCards.Ren...			C:\Windows\SystemApps\MicrosoftWindows.Client.Core_cw...

CPU Usage: 5.86% Commit Charge: 43.49% Processes: 269 Physical Usage: 68.32%

Рис. 14. Список разделяемых библиотек, используемых конкретным процессом

Диспетчер задач

Ведите имя, издателя или PI...

Процессы

Запустить новую задачу

Процессы

Производительность

Журнал приложений

Автозагрузка приложений

Пользователи

Сведения

Службы

Параметры

Имя Состояние 4% ЦП 70% Память

Приложения (9)

- > Google Chrome (20) 0% 2 173,9 МБ
- > Microsoft Word (2) 0% 125,8 МБ
- > MSYS2 terminal 0% 1,9 МБ
- > Notepad.exe 0% 14,0 МБ
- > Sysinternals Process Explorer 0% 28,2 МБ
- > Telegram Desktop 0% 115,3 МБ
- > VirtualBox Manager 0% 16,0 МБ
- > Диспетчер задач 1,0% 93,4 МБ
- > Проводник (3) 0% 160,9 МБ

Фоновые процессы (93)

- > Acrobat Update Service (32 бит) 0% 0,3 МБ
- > Adobe IPC Broker (32 бита) 0% 1,0 МБ
- > Antimalware Core Service 0% 4,9 МБ

Рис. 15

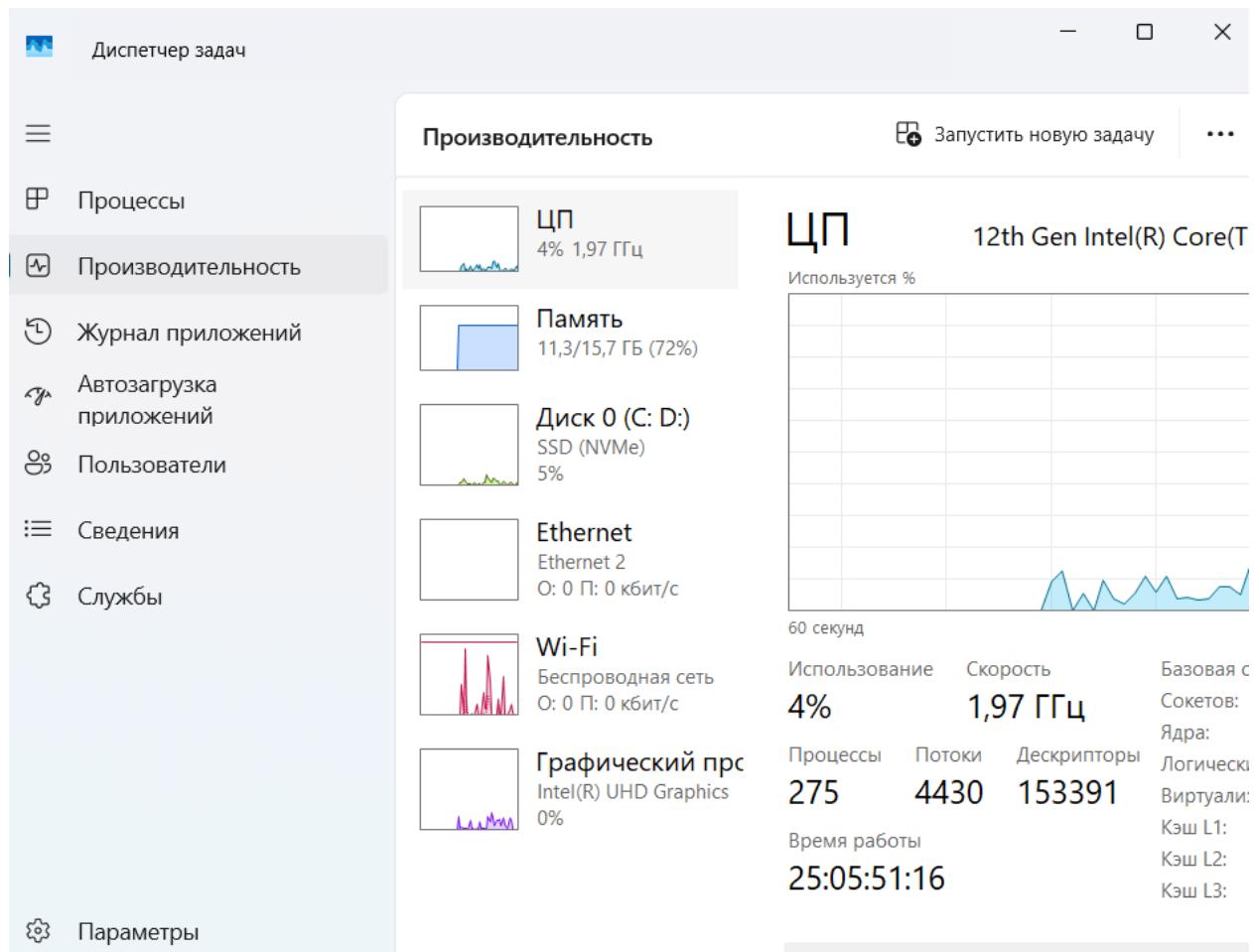


Рис. 16

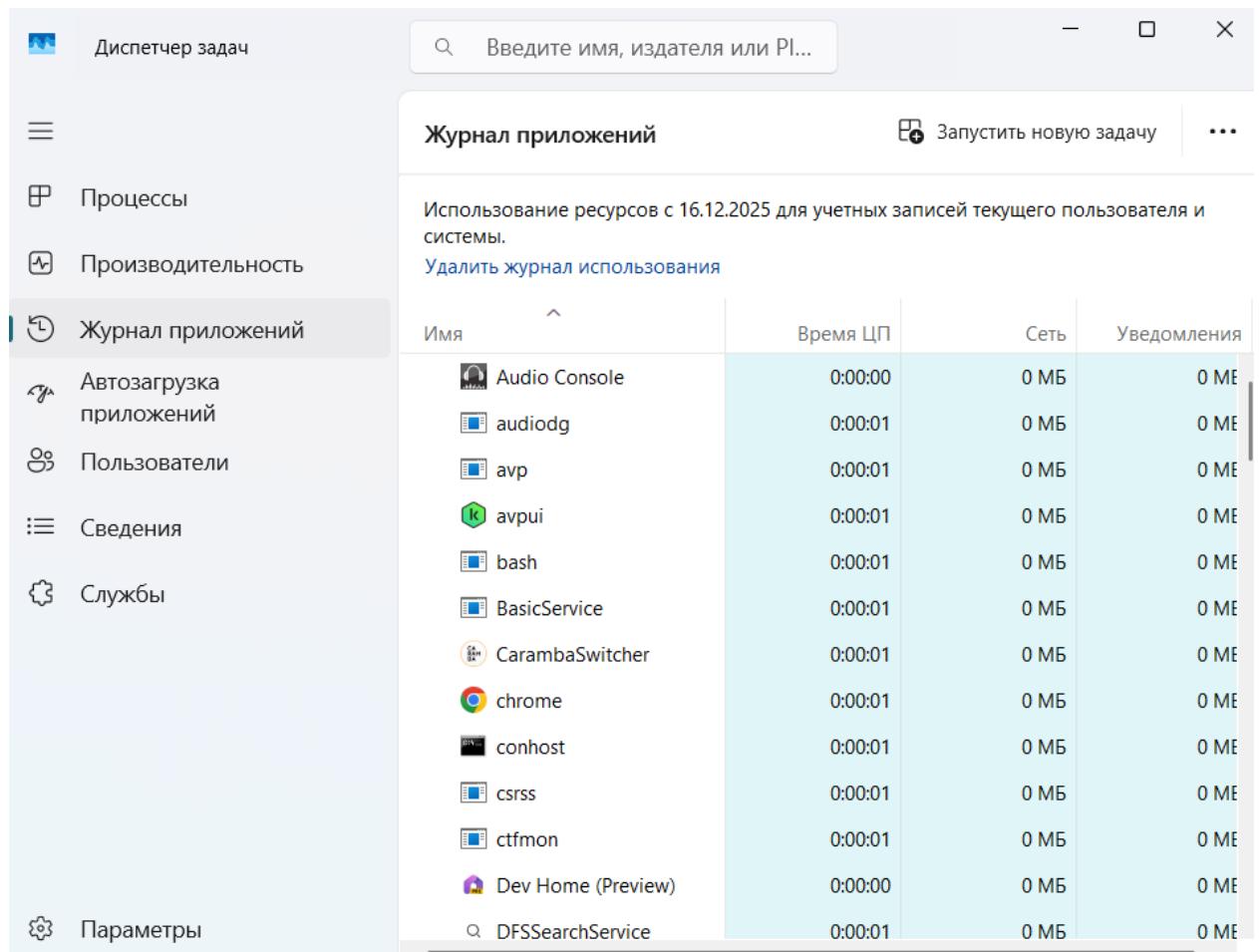


Рис. 17

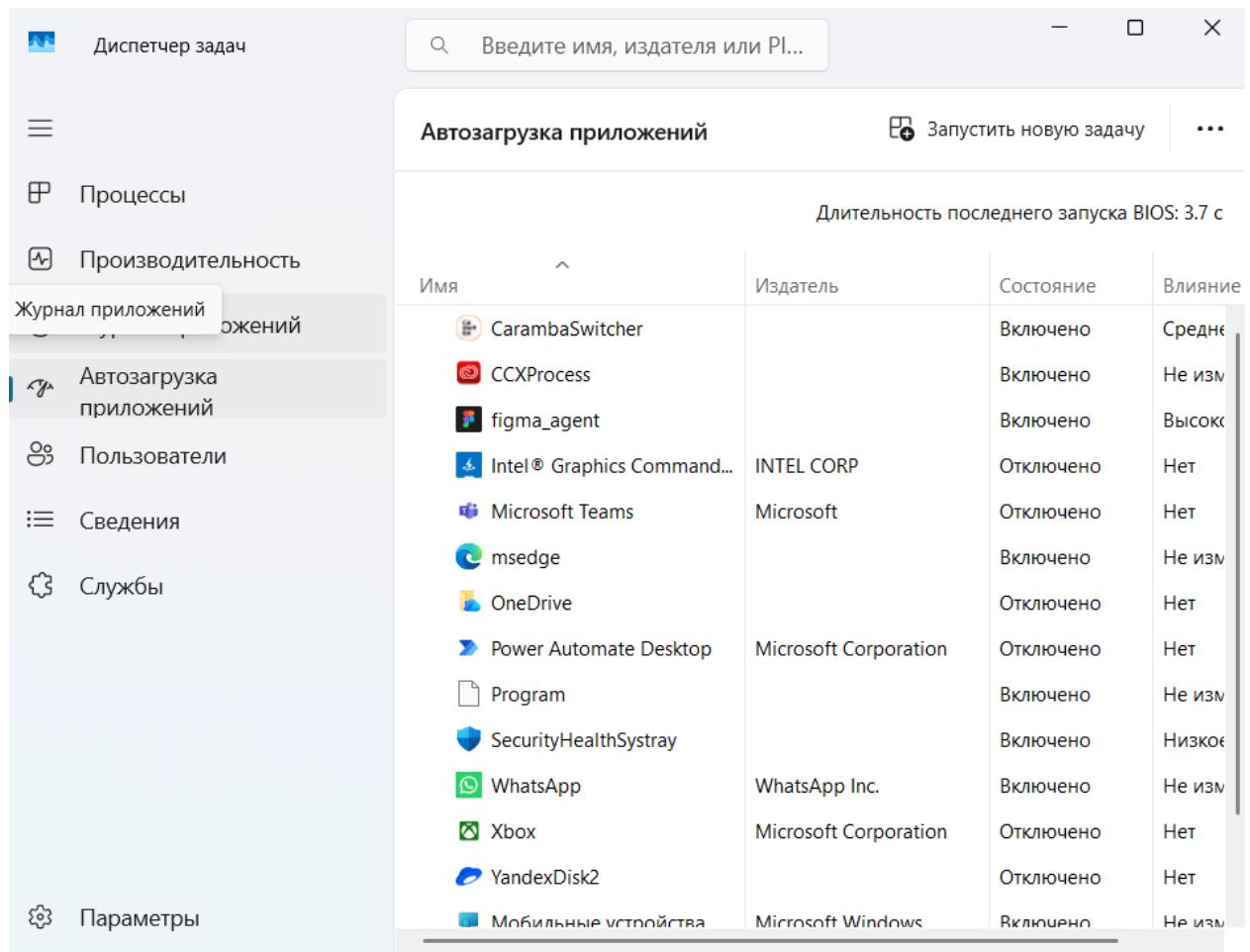


Рис. 18

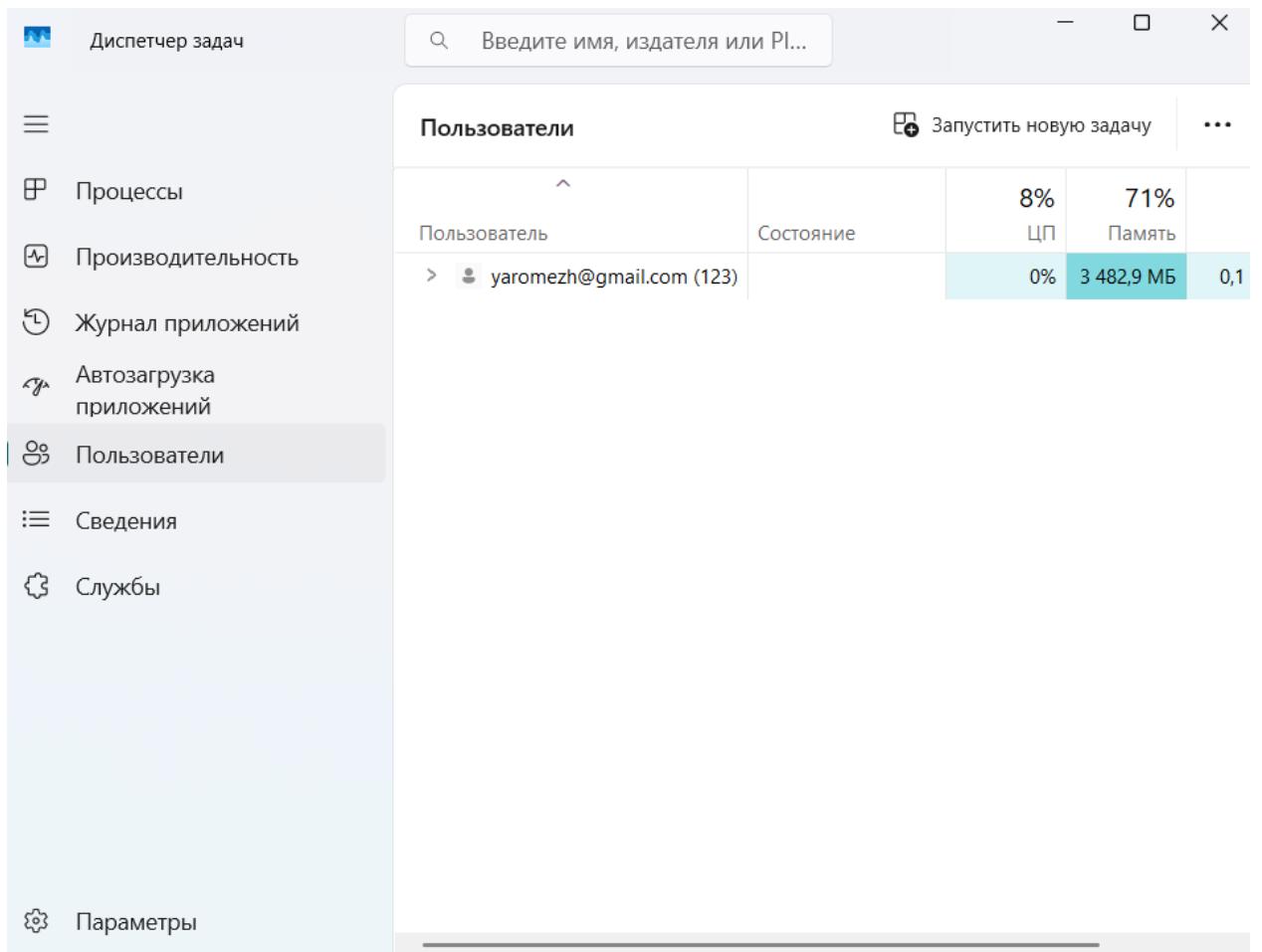


Рис. 19

Диспетчер задач

Введите имя, издателя или PI...

Сведения

Запустить новую задачу

...

Процессы Имя ИД п... Состо... Имя польз... ЦП Дельт... Платфо... Вирту

Производительность AdobelPCBroker.exe 23628 Выпол... yarom 00 0 K 32 бита Откл.

Журнал приложений AggregatorHost.exe 8936 Выпол... СИСТЕМА 00 0 K 64 бита Не р.

Автозагрузка приложений ApplicationFrameHo... 16392 Выпол... yarom 00 0 K 64 бита Откл.

Пользователи armsvc.exe 4384 Выпол... СИСТЕМА 00 0 K 32 бита Не р.

Сведения audiogd.exe 19376 Выпол... LOCAL SER... 00 0 K 64 бита Не р.

Службы avp.exe 4744 Выпол... СИСТЕМА 00 0 K 32 бита Не р.

Параметры avp.exe 8952 Выпол... СИСТЕМА 00 0 K 32 бита Не р.

Службы avpui.exe 16688 Выпол... yarom 00 0 K 32 бита Откл.

Службы backgroundTaskHost... 15700 Выпол... yarom 00 0 K 64 бита Откл.

Службы bash.exe 24676 Выпол... yarom 00 0 K 64 бита Откл.

Службы BasicService.exe 4632 Выпол... СИСТЕМА 00 0 K 64 бита Не р.

Службы CarambaSwitcher.exe 6792 Выпол... yarom 00 0 K 32 бита Откл.

Службы CCXProcess.exe 7720 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 28136 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 16580 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 13772 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 27812 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 22808 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 13076 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 18292 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 24624 Выпол... yarom 00 0 K 64 бита Откл.

Службы chrome.exe 9824 Выпол... yarom 00 0 K 64 бита Откл.

Рис. 20

Диспетчер задач

Ведите имя, издателя или PI...

Службы

Запустить новую задачу

...

☰

	Имя	Ид ...	Описание	Состояние	Группа
⊕ Процессы	AarSvc_3bbf97ad	4384	Agent Activ...	Остановле...	AarSvcGroup
〽 Производительность	AdobeARMservice		Adobe Acro...	Выполняет...	
⌚ Журнал приложений	ADPSvc		Служба пл...	Остановле...	LocalServic...
🔧 Автозагрузка приложений	ALG		Служба шл...	Остановле...	
⟳ Пользователи	AppHostSvc	4420	Служба по...	Выполняет...	apphost
⟳ Сведения	AppIDSvc	1876	Удостовере...	Выполняет...	LocalServic...
👤 Службы	Appinfo	8104	Сведения о...	Выполняет...	netsvcs
	AppReadiness		Готовность...	Остановле...	AppReadin...
	AppXSvc	6796	Служба ра...	Выполняет...	wsappx
	ApxSvc		Прокси-слу...	Остановле...	LocalService
	aspnet_state		ASP.NET St...	Остановле...	
	AudioEndpointBuilder	3304	Средство п...	Выполняет...	LocalSyste...
	Audiosrv	3412	Windows A...	Выполняет...	LocalServic...
	autotimesvc		Время в се...	Остановле...	autoTimeSvc
	AVP21.23	4744	Kaspersky S...	Выполняет...	
	AxInstSV		Установщи...	Остановле...	AxInstSVGr...
	BcastDVRUserService_3...		Пользоват...	Остановле...	BcastDVRU...
	BDESVC		Служба ши...	Остановле...	netsvcs
	BFE	3948	Служба ба...	Выполняет...	LocalServic...
	BITS		Фоновая и...	Остановле...	netsvcs
	BluetoothUserService_3...	8504	Служба по...	Выполняет...	BthAppGro...

⚙️ Параметры

Рис. 21

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks Appinit

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms				01.04.2024 10:26	
rdpcdr	Монитор буфера обмена R...	Microsoft Corporation	c:\windows\system32\rdpcdr...	06.07.1958 15:43	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	C:\Windows\syst... Приложение Userinit для вх...	Microsoft Corporation	c:\windows\system32\userinit...	15.01.2026 10:27	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet				13.07.1948 14:49	
SystemProperties...	Изменение параметров пр...	Microsoft Corporation	c:\windows\system32\system...	15.01.2026 10:27	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				18.06.1912 5:47	
explorer.exe	Проводник	Microsoft Corporation	c:\windows\explorer.exe	15.01.2026 10:27	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				19.09.1987 3:34	
cmd.exe	Обработчик команд Windo...	Microsoft Corporation	c:\windows\system32\cmd.exe	10.04.1995 17:13	
HKLM\Software\Microsoft\Windows\CurrentVersion\Run				01.04.2024 10:28	
SecurityHealth	Windows Security notification ...	Microsoft Corporation	c:\windows\system32\security...	01.04.2024 10:28	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				27.10.1946 22:04	
Adobe CCXProc...			c:\program files (x86)\adobe\...	14.11.2025 10:28	
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				05.01.2021 0:35	
CarambaSwitcher	Caramba Switcher	Caramba Switcher	c:\program files (x86)\caramb...	08.01.2026 9:12	
Figma Agent	Figma Agent	Figma Agent	c:\users\yarom\appdata\local...	16.12.2024 16:30	
MicrosoftEdgeAu...	Microsoft Edge	Microsoft Corporation	c:\program files (x86)\microso...	02.12.2025 20:29	
OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\yarom\appdata\local...	08.01.2026 9:34	
YandexDisk2	Яндекс.Диск	Яндекс	c:\users\yarom\appdata\roa...	12.11.2037 19:13	
YandexDisk2	Яндекс.Диск	Яндекс	c:\users\yarom\appdata\roa...	14.08.2025 15:00	
C:\Users\yarom\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Отправка в One...		File not found: File	18.11.2025 11:44	
HKLM\Software\Microsoft\Active Setup\Installed Components				20.11.2025 19:54	
Google Chrome	Google Chrome Installer	Google LLC	c:\program files\google\chrom...	06.01.2026 2:00	
Google Platform	Google Chrome	Google LLC	c:\program files\google\chrom...	06.11.2025 8:01	
Microsoft Edge	Microsoft Edge Installer	Microsoft Corporation	c:\program files (x86)\microso...	08.01.2026 9:34	
Microsoft Windows	Программа установки тра...	Microsoft Corporation	c:\windows\system32\unregm...	08.07.1982 2:20	
Microsoft Windows	Программа установки тра...	Microsoft Corporation	c:\windows\system32\unregm...	08.07.1982 2:20	

Ready. | No Filter.

Рис. 22. Вкладка Logon

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit

Autorun Entry **Description** **Publisher** **Image Path** **Timestamp** **VirusTotal**

HKLM\System\CurrentControlSet\Services 15.01.2026 14:31

AairSvc	Runtime for activating conver...	Microsoft Corporation	c:\windows\system32\aaarsvc...	20.12.1987 3:02	
AarSvc_3bbf97ad	Runtime for activating conver...	Microsoft Corporation	c:\windows\system32\svchost...	21.06.1970 6:53	
AdobeARMservi...	Adobe Acrobat Updater keep...	Adobe Inc.	c:\program files (x86)\commo...	25.08.2025 4:19	
ADPSvc	Эта служба используетс...	Microsoft Corporation	c:\windows\system32\adpsvc...	18.04.1975 3:15	
ALG	Обеспечивает поддержку ...	Microsoft Corporation	c:\windows\system32\alg.exe	03.05.2008 13:58	
AppHostSvc	Является административн...	Microsoft Corporation	c:\windows\system32\inetsrv...	06.03.2030 1:23	
AppIDSvc	Определяет и проверяет у...	Microsoft Corporation	c:\windows\system32\appids...	19.05.1913 2:17	
Appinfo	Обеспечивает выполнени...	Microsoft Corporation	c:\windows\system32\appinfo...	28.04.1957 1:57	
AppReadiness	Подготовка приложений к ...	Microsoft Corporation	c:\windows\system32\apprea...	13.04.1954 10:46	
AppXSvc	Обеспечивает поддержку ...	Microsoft Corporation	c:\windows\system32\appxde...	07.06.1905 1:18	
ApxSvc	Управляет виртуальными ...	Microsoft Corporation	c:\windows\system32\apxsvc...	19.05.1956 6:02	
aspnet_state	Provides support for out-of-pr...	Microsoft Corporation	c:\windows\microsoft\netfram...	18.06.2025 23:26	
AudioEndpointBu...	Управление звуковыми ус...	Microsoft Corporation	c:\windows\system32\audioe...	27.02.2025 8:47	
Audiosrv	Управление средствами р...	Microsoft Corporation	c:\windows\system32\audiosr...	08.08.1936 6:42	
autotimesvc	Эта служба устанавливает...	Microsoft Corporation	c:\windows\system32\autotim...	29.05.1974 6:25	
AVP21.23	Обеспечивает защиту ком...	AO Kaspersky Lab	c:\program files (x86)\kaspers...	10.06.2025 18:00	
AxInstSV	Обеспечивает проверку к...	Microsoft Corporation	c:\windows\system32\axinsts...	22.01.1998 22:37	
BcastDVRUserS...	Эта пользовательская слу...	Microsoft Corporation	c:\windows\system32\bcastd...	26.01.2007 8:00	
BcastDVRUserS...	Эта пользовательская слу...	Microsoft Corporation	c:\windows\system32\svchost...	21.06.1970 6:53	
BDESVC	BDESVC предоставляет сл...	Microsoft Corporation	c:\windows\system32\bdesvc...	16.04.2023 21:59	
BFE	Служба базовой фильтрац...	Microsoft Corporation	c:\windows\system32\bfe.dll	11.10.1993 21:11	
BITS	Передает файлы в фоново...	Microsoft Corporation	c:\windows\system32\qmgr.dll	19.08.2035 23:39	
BluetoothUserSe...	Служба поддержки пользо...	Microsoft Corporation	c:\windows\system32\micros...	02.02.1969 11:41	
BluetoothUserSe...	Служба поддержки пользо...	Microsoft Corporation	c:\windows\system32\svchost...	21.06.1970 6:53	
BrokerInstructu...	Служба инфраструктуры ...	Microsoft Corporation	c:\windows\system32\psmsrv...	23.01.2017 11:39	
BTAGService	Служба, поддерживающая ...	Microsoft Corporation	c:\windows\system32\btagserv...	25.02.2019 9:05	
RthAvctnSvc	Это служба протокола тра...	Microsoft Corporation	c:\windows\system32\lthavct...	31.12.1938 20:57	

Ready. | No Filter. |

Рис. 23. Вкладка **Scheduled Tasks**

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office

Autorun Entry Description Publisher Image Path Timestamp VirusTotal

HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers				01.04.2024 10:28	
✓ %windir%\system... "RdpCredentialProvider.DYN..." Microsoft Corporation	c:\windows\system32\rdpcred...	11.06.1965 12:02			
✓ Automatic Redep... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\mgmtre...	30.05.1997 18:59			
✓ CCertProvider Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\certcre...	02.05.2007 13:16			
✓ Cloud Experienc... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\cxcred...	28.03.1937 7:05			
✓ CngCredUICrede... Поставщик Microsoft CNG Cr... Microsoft Corporation	c:\windows\system32\cngcre...	18.03.1939 9:49			
✓ FaceCredentialPr... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\facecre...	09.09.1918 23:53			
✓ FIDO Credential ... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\fidocre...	25.02.1970 11:36			
✓ GenericProvider Поставщики учетных данны... Microsoft Corporation	c:\windows\system32\credpro...	22.12.1989 6:43			
✓ NGC Credential P... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\ngccre...	09.12.1970 6:05			
✓ NPPProvider Поставщики учетных данны... Microsoft Corporation	c:\windows\system32\credpro...	22.12.1989 6:43			
✓ PasswordProvider Поставщики учетных данны... Microsoft Corporation	c:\windows\system32\credpro...	22.12.1989 6:43			
✓ PicturePassword... Устаревшие поставщики у... Microsoft Corporation	c:\windows\system32\credpro...	13.01.1997 14:01			
✓ PINLogonProvider Устаревшие поставщики у... Microsoft Corporation	c:\windows\system32\credpro...	13.01.1997 14:01			
✓ Second Authentic... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\device...	04.12.1902 5:22			
✓ Smartcard Credet... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\smartc...	04.12.2020 1:47			
✓ Smartcard Pin Pr... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\smartc...	04.12.2020 1:47			
✓ Smartcard Read... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\smartc...	04.12.2020 1:47			
✓ Smartcard WinR... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\smartc...	04.12.2020 1:47			
✓ TrustedSignal Cr... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\trusted...	21.08.1985 14:57			
✓ WinBio Credential... Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\biocred...	12.07.1928 14:36			
✓ WLICredentialP... Microsoft® Account Credential... Microsoft Corporation	c:\windows\system32\wlidcre...	16.04.1961 2:51			
HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters			01.04.2024 10:28		
✓ GenericFilter Поставщики учетных данны... Microsoft Corporation	c:\windows\system32\credpro...	22.12.1989 6:43			
HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers			01.04.2024 10:28		
✓ CRasProvider Поставщик учетных данны... Microsoft Corporation	c:\windows\system32\raslap...	23.05.1922 9:17			
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions			01.04.2024 19:32		
✓ (0ACDD40C-75A_ Клиент групповой политик Microsoft Corporation	c:\windows\system32\wlgpcnt.dll	4.08.1924 6:07			

Ready. | No Filter.

Рис. 24. Вставка Services

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit

Autorun Entry Description Publisher Image Path Timestamp VirusTotal

Task Scheduler

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
Adobe Acrobat...	Adobe Reader and Acrobat ...	Adobe Inc.	c:\program files (x86)\commo...	25.08.2025 4:20	
\CreateExplorerS...	Проводник	Microsoft Corporation	c:\windows\explorer.exe	19.09.1987 3:34	
\Microsoft\Office\...	Microsoft Office Click-to-Run ...	Microsoft Corporation	c:\program files\common files...	04.08.2022 23:10	
\Microsoft\Office\...	Microsoft Office Click-to-Run ...	Microsoft Corporation	c:\program files\common files...	04.08.2022 23:10	
\Microsoft\Office\...	Microsoft Office SDX Helper	Microsoft Corporation	c:\program files\microsoft offic...	04.08.2022 23:29	
\Microsoft\Office\...	Microsoft Office SDX Helper	Microsoft Corporation	c:\program files\microsoft offic...	04.08.2022 23:29	
\Microsoft\Office\...	Office Telemetry Dashboard ...	Microsoft Corporation	c:\program files\microsoft offic...	04.08.2022 23:32	
\Microsoft\Office\...	Office Telemetry Dashboard ...	Microsoft Corporation	c:\program files\microsoft offic...	04.08.2022 23:32	
\Microsoft\Visual...	Visual Studio Background Do...	Microsoft	c:\program files (x86)\microso...	09.11.1903 15:58	
\Microsoft\Windo...	Microsoft .NET Runtime Exec...	Microsoft Corporation	c:\windows\system32\mscore...	20.10.1970 17:22	
\Microsoft\Windo...	Microsoft .NET Runtime Exec...	Microsoft Corporation	c:\windows\system32\mscore...	20.10.1970 17:22	
\Microsoft\Windo...	Microsoft .NET Runtime Exec...	Microsoft Corporation	c:\windows\system32\mscore...	20.10.1970 17:22	
\Microsoft\Windo...	AccountHealth	Microsoft Corporation	c:\windows\system32\account...	20.10.1958 9:04	
\Microsoft\Windo...	Клиент управления правами	Microsoft Corporation	c:\windows\system32\msdm...	10.04.1933 16:53	
\Microsoft\Windo...	Клиент управления правами	Microsoft Corporation	c:\windows\system32\msdm...	10.04.1933 16:53	
\Microsoft\Windo...	AppID Policy Converter Task	Microsoft Corporation	c:\windows\system32\appidp...	15.07.1937 20:50	
\Microsoft\Windo...	AppID Certificate Store Verific...	Microsoft Corporation	c:\windows\system32\appidc...	31.01.2001 17:20	
\Microsoft\Windo...	Телеметрия совместимости...	Microsoft Corporation	c:\windows\system32\compat...	21.04.2033 16:21	
\Microsoft\Windo...	Телеметрия совместимости...	Microsoft Corporation	c:\windows\system32\compat...	21.04.2033 16:21	
\Microsoft\Windo...	Телеметрия совместимости...	Microsoft Corporation	c:\windows\system32\compat...	21.04.2033 16:21	
\Microsoft\Windo...	Служба помощника по совместим...	Microsoft Corporation	c:\windows\system32\pcasvc...	17.06.1911 19:36	
\Microsoft\Windo...	Установщик базы данных ...	Microsoft Corporation	c:\windows\system32\sdbinst...	17.06.1966 23:23	
\Microsoft\Windo...	Библиотека DLL задачи сканиров...	Microsoft Corporation	c:\windows\system32\startups...	16.05.1940 1:07	
\Microsoft\Windo...	Средство проверки регистров...	Microsoft Corporation	c:\windows\system32\apphos...	16.11.1935 18:23	
\Microsoft\Windo...	Средство проверки регистра...	Microsoft Corporation	c:\windows\system32\annhos...	16.11.1935 18:23	

Ready. | No Filter. [x]

Рис. 25. Вставка Winlogon

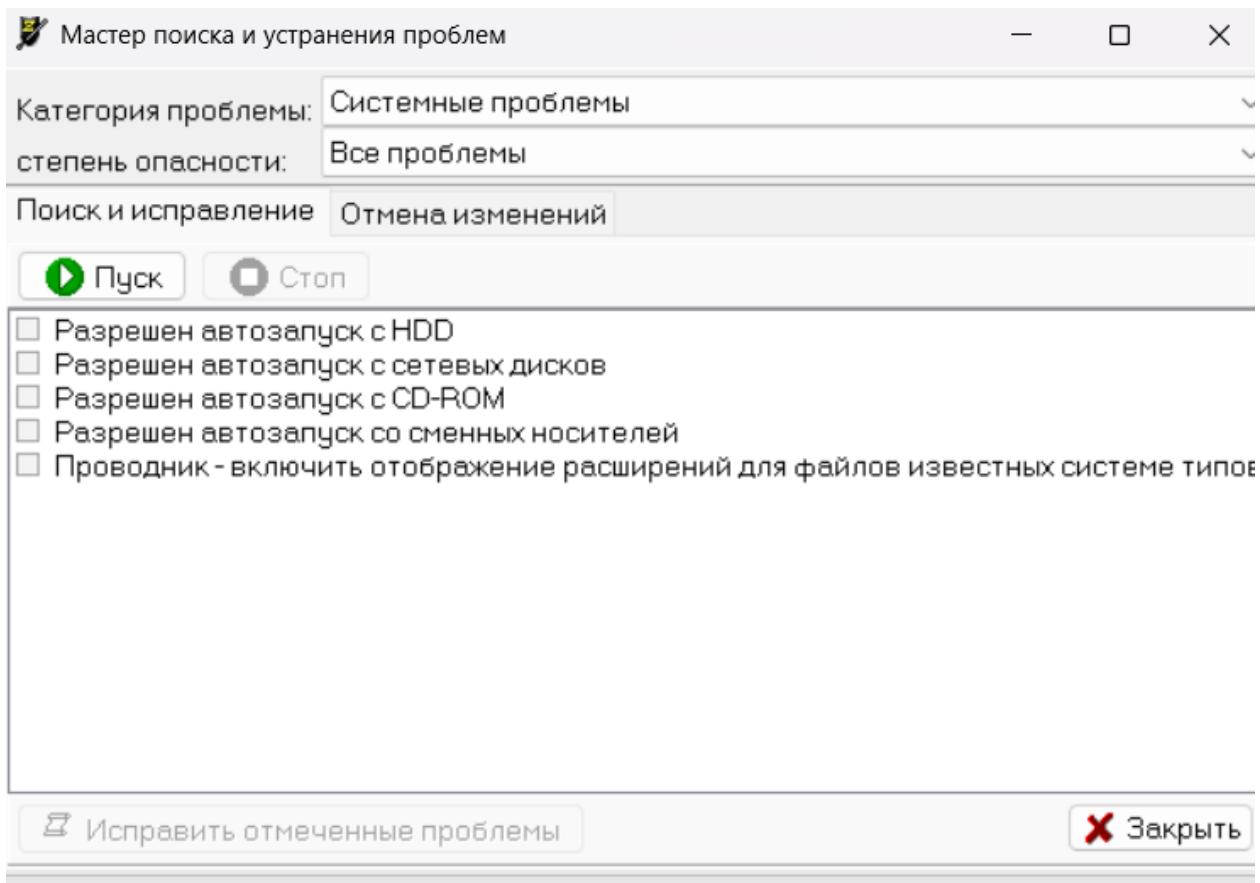


Рис. 26

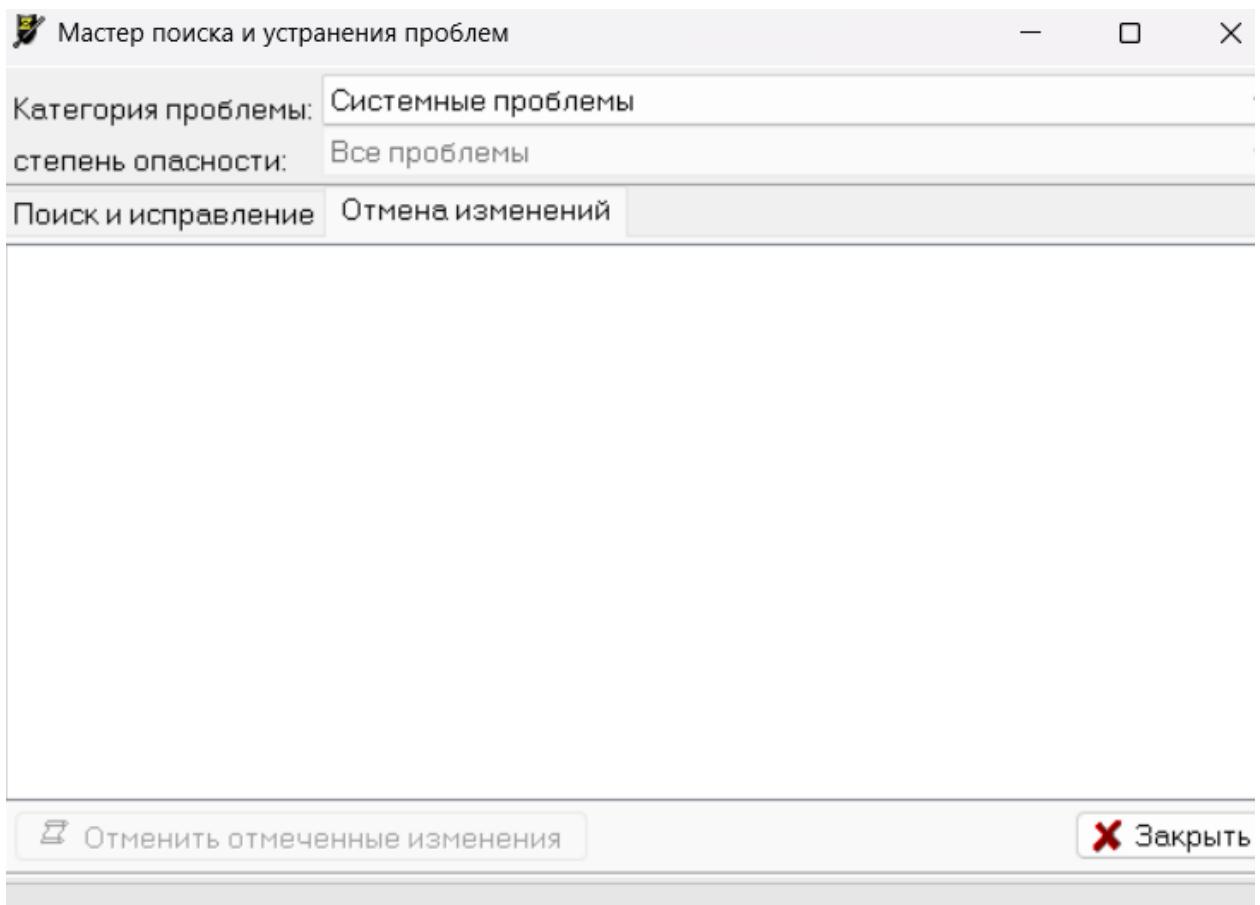


Рис. 27. Получите информацию об имеющихся в ОС проблемах

```
Сканирование выполнено
Версия Windows: 10.0.26200, "Windows 10 Home", дата инсталляции 14.11.2025 10:33:25 ; AVZ работает
Восстановление системы: включено
1. Поиск RootKit и программ, перехватывающих функции API
1.1 Поиск перехватчиков API, работающих в UserMode
Анализ kernel32.dll, таблица экспорта найдена в секции .rdata
Функция kernel32.dll:ReadConsoleInputExA (1180) перехвачена, метод ProcAddressHijack.GetProcAddress
Функция kernel32.dll:ReadConsoleInputExW (1181) перехвачена, метод ProcAddressHijack.GetProcAddress
Анализ ntdll.dll, таблица экспорта найдена в секции .text
Функция ntdll.dll:NtCreateFile (307) перехвачена, метод ProcAddressHijack.GetProcAddress ->77C3948
Функция ntdll.dll:NtSetInformationFile (620) перехвачена, метод ProcAddressHijack.GetProcAddress ->7
```

Рис. 28. Антивирусное сканирование системы

Контрольные вопросы:

1. Информации о службах
 - Запустить оснастку services.msc через меню Пуск - Выполнить
2. Древовидный режим в Process Explorer:
 - Меню View - Show Process Tree или клавиши.
3. Отображение нижней панели:
 - Включить/выключить через меню View - Show Lower Pane или клавиши.
4. Процесс с наибольшим CPU:
 - Нажать на заголовок столбца CPU для сортировки по убыванию.
5. Процесс с наибольшей RAM:
 - Нажать на заголовок столбца Working Set для сортировки.
6. Наибольшее чтение данных (I/O Read):
 - Включить столбец I/O Read Bytes через Select Columns - вкладка Process I/O и отсортировать по нему.
7. Наибольшая запись данных (I/O Write):
 - Включить и отсортировать столбец I/O Write Bytes.
8. Количество ядер процессора:
 - Открыть View - System Information, информация доступна на вкладках Summary или CPU.
9. Объем оперативной памяти:
 - Открыть System Information на вкладке Memory.

10. Суммарный процент использования CPU:

- Посмотреть в статусной строке в нижней части главного окна программы.

11. Процент RAM и файла подкачки:

- Посмотреть в статусной строке (второй индикатор внизу окна).

12. Общее количество процессов:

- Указано в статусной строке внизу (надпись Processes).

13. Суммарный процент использования RAM:

- Указано в статусной строке (крайний правый индикатор).

14. Путь к исполняемому файлу:

- Двойной щелчок по процессу - вкладка Image, строка Path.

15. Имя пользователя:

- В свойствах процесса (Image) в строке User.

16. Время запуска процесса:

- В свойствах процесса (Image) в строке Started.

17. Список служб процесса:

- Двойной щелчок по процессу - вкладка Services.

18. Поиск процессов по библиотеке (DLL):

- Меню Find - Find Handle or DLL, ввести имя DLL и нажать Search.

19. Список библиотек конкретного процесса:

- Выбрать процесс и нажать View - Lower Pane View - DLLs).

20. Сканирование VirusTotal:

- Меню Options - VirusTotal.com - Check VirusTotal.com, затем Submit Unknown Executables.

21. Информация об автозапуске:

- Запустить autoruns.exe и дождаться статуса "Ready". Вкладка Everything покажет все объекты.

22. Сканирование автозапуска на VirusTotal:

- Меню Options - Scan Options - Check VirusTotal.com, нажать Rescan.

23. Поиск системных проблем в AVZ:

- Меню Файл - Исследование системы или Файл - Восстановление системы.

24. Антивирусное сканирование в AVZ:

- Выбрать области поиска в левой части окна, задать методику лечения и нажать кнопку Пуск.