



ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ

ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное

образовательное учреждение города Москвы

«Колледж малого бизнеса № 4»

(ГБПОУ КМБ № 4)

Отчёт попрактической 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.

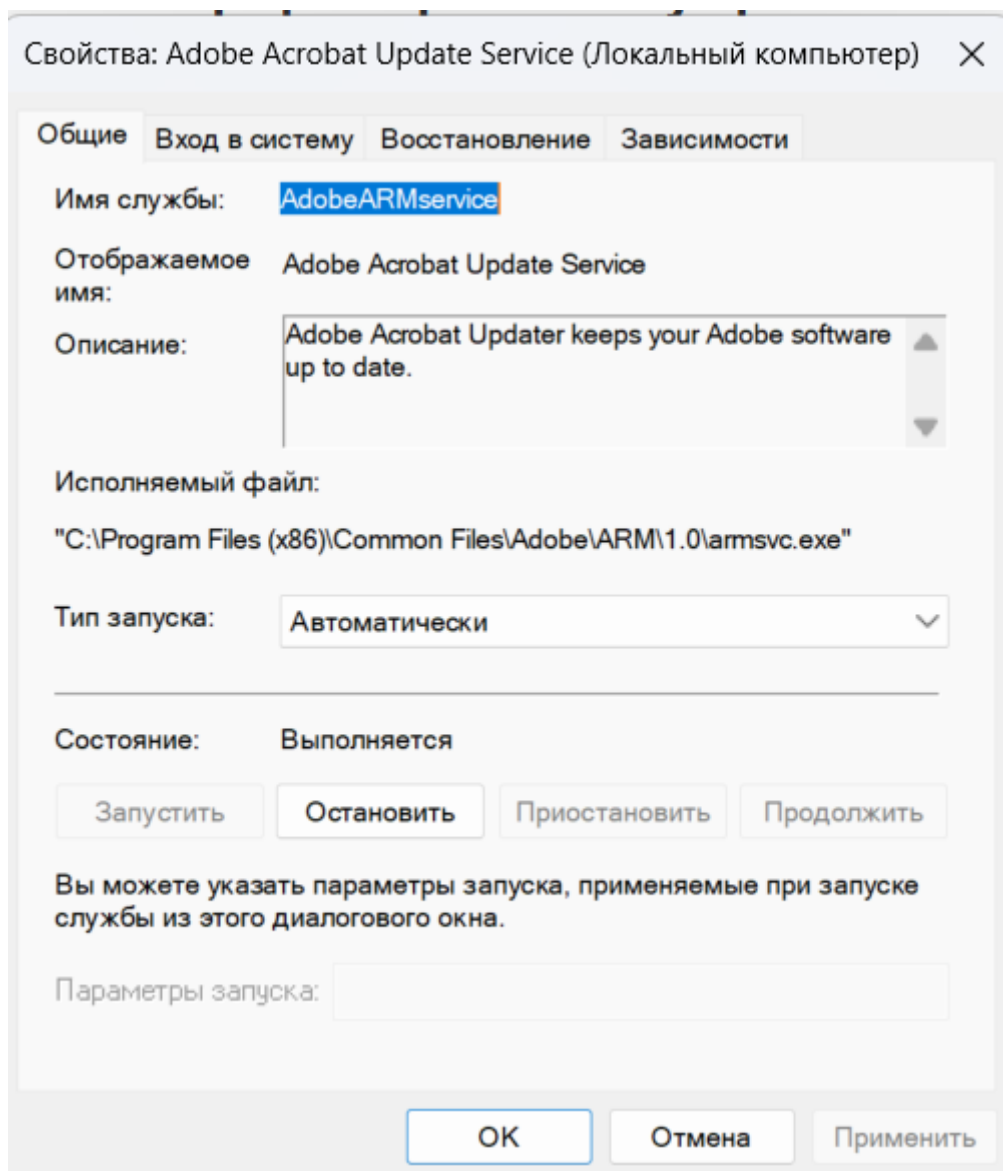


Рис. 1. Сортировка служб по состоянию после нажатия на Состояния

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

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|-----------------------------|---------|---------------|-------------|-------|-------------------------------|-----------------------|
| Secure System | Susp... | 172 K | 63 628 K | 188 | | |
| Registry | | 13 536 K | 53 184 K | 232 | | |
| System Idle Process | 97.43 | 60 K | 8 K | 0 | | |
| System | 0.27 | 56 K | 1 108 K | 4 | | |
| Interrupts | 0.28 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1 180 K | 652 K | 880 | | |
| Memory Compression | | 3 952 K | 783 756 K | 3224 | | |
| csrss.exe | | 2 716 K | 4 048 K | 1124 | | |
| wininit.exe | | 1 932 K | 4 108 K | 1208 | | |
| services.exe | | 6 676 K | 9 044 K | 1352 | | |
| svchost.exe | < 0.01 | 44 012 K | 48 540 K | 1568 | Хост-процесс для служб W... | Microsoft Corporation |
| unsecapp.exe | | 2 208 K | 3 544 K | 6892 | | |
| WmiPrvSE.exe | | 45 068 K | 15 284 K | 6920 | | |
| unsecapp.exe | | 2 572 K | 12 064 K | 21124 | | |
| StartMenuExperienceHost.exe | | 91 660 K | 162 756 K | 7796 | Windows Start Experience H... | Microsoft Corporation |
| RuntimeBroker.exe | | 17 112 K | 68 476 K | 20768 | Runtime Broker | Microsoft Corporation |
| Widgets.exe | | 12 532 K | 68 780 K | 15960 | | Microsoft Corporation |
| msedgewebview2.exe | | 41 356 K | 12 412 K | 29592 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 2 312 K | 9 316 K | 13744 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 89 132 K | 6 524 K | 19876 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 13 104 K | 6 264 K | 6564 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 10 124 K | 3 160 K | 19248 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 69 164 K | 4 852 K | 11368 | Microsoft Edge WebView2 | Microsoft Corporation |
| ShellExperienceHost.exe | Susp... | 70 660 K | 121 584 K | 16228 | Windows Shell Experience H... | Microsoft Corporation |
| TextInputHost.exe | | 124 392 K | 180 112 K | 5712 | | Microsoft Corporation |
| SearchHost.exe | | 91 876 K | 171 772 K | 7188 | | Microsoft Corporation |
| msedgewebview2.exe | | 43 016 K | 114 168 K | 4264 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 2 368 K | 9 008 K | 25456 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 139 164 K | 81 200 K | 26156 | Microsoft Edge WebView2 | Microsoft Corporation |
| msedgewebview2.exe | | 14 436 K | 40 708 K | 9780 | Microsoft Edge WebView2 | Microsoft Corporation |

CPU Usage: 2.57% Commit Charge: 41.28% Processes: 268 Physical Usage: 67.97%

Рис. 2. Показ дерева процессов в Process Explorer

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

File Options View Process Find Users Help

| 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 L... | 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]

File Options View Process Find Users Help

| 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

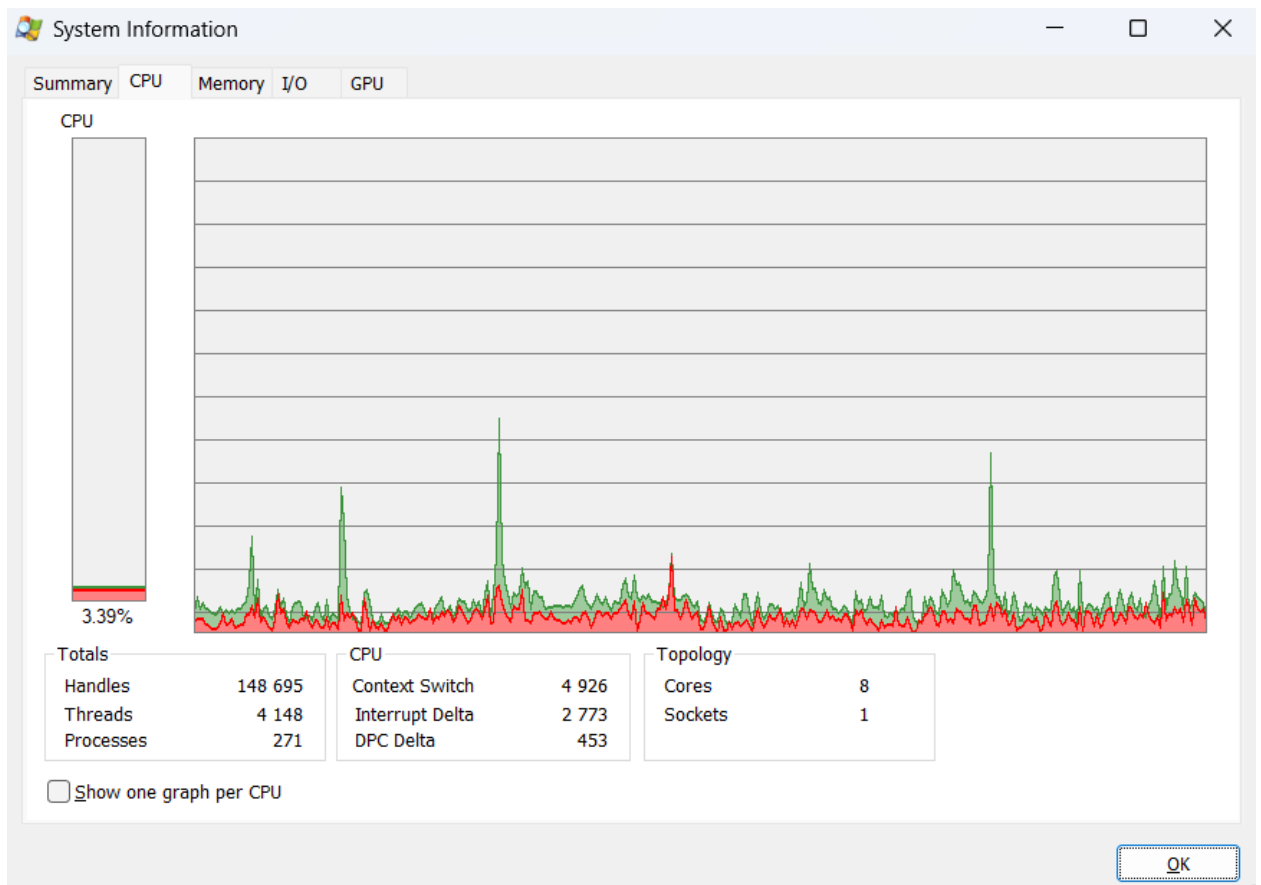
Process Explorer - Sysinternals: www.sysinternals.com [HUAWEI_LAPTOP\yarom]

File Options View Process Find Users Help

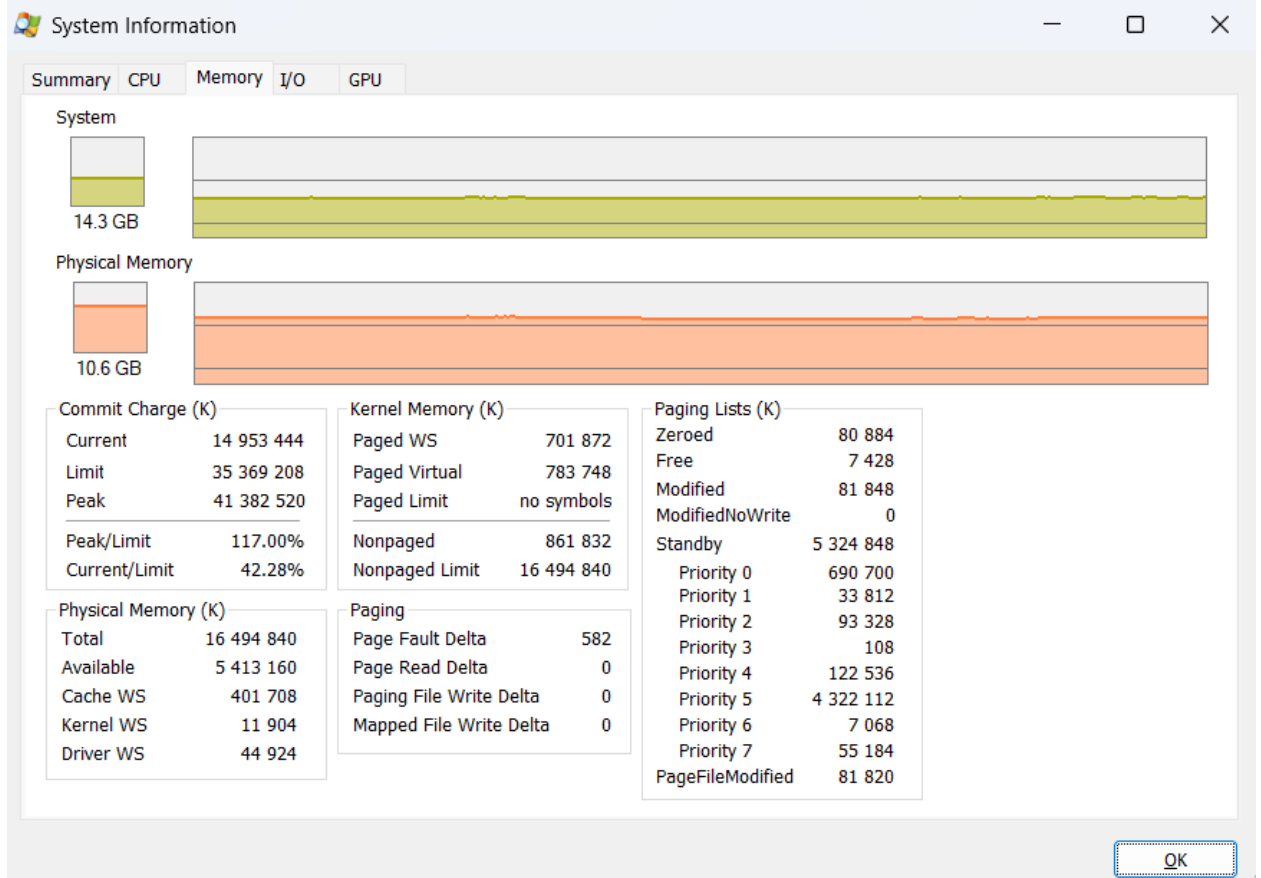
| Process | Working Set | PID | Description | Company Name | I/O Read Bytes | I/O Write Bytes |
|----------------------------|-------------|-------|-------------------------------------|-------------------------|----------------|-----------------|
| Intel_PIE_Service.exe | 2 844 K | 10020 | SHA1:0xefecbf60 | Intel Corporation | | |
| IntelAudioService.exe | 7 004 K | 4504 | IntelAudioService | Intel | | |
| IntelCpHDCCSvc.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 Executa... | Microsoft Corporation | | |
| mysqld.exe | 3 168 K | 4836 | | Oracle Corporation | | |
| mysqld.exe | 3 684 K | 5428 | | | | |
| Ngclso.exe | 2 228 K | 4152 | | | | |
| NisSrv.exe | 5 684 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



Puc. 7



Puc. 8

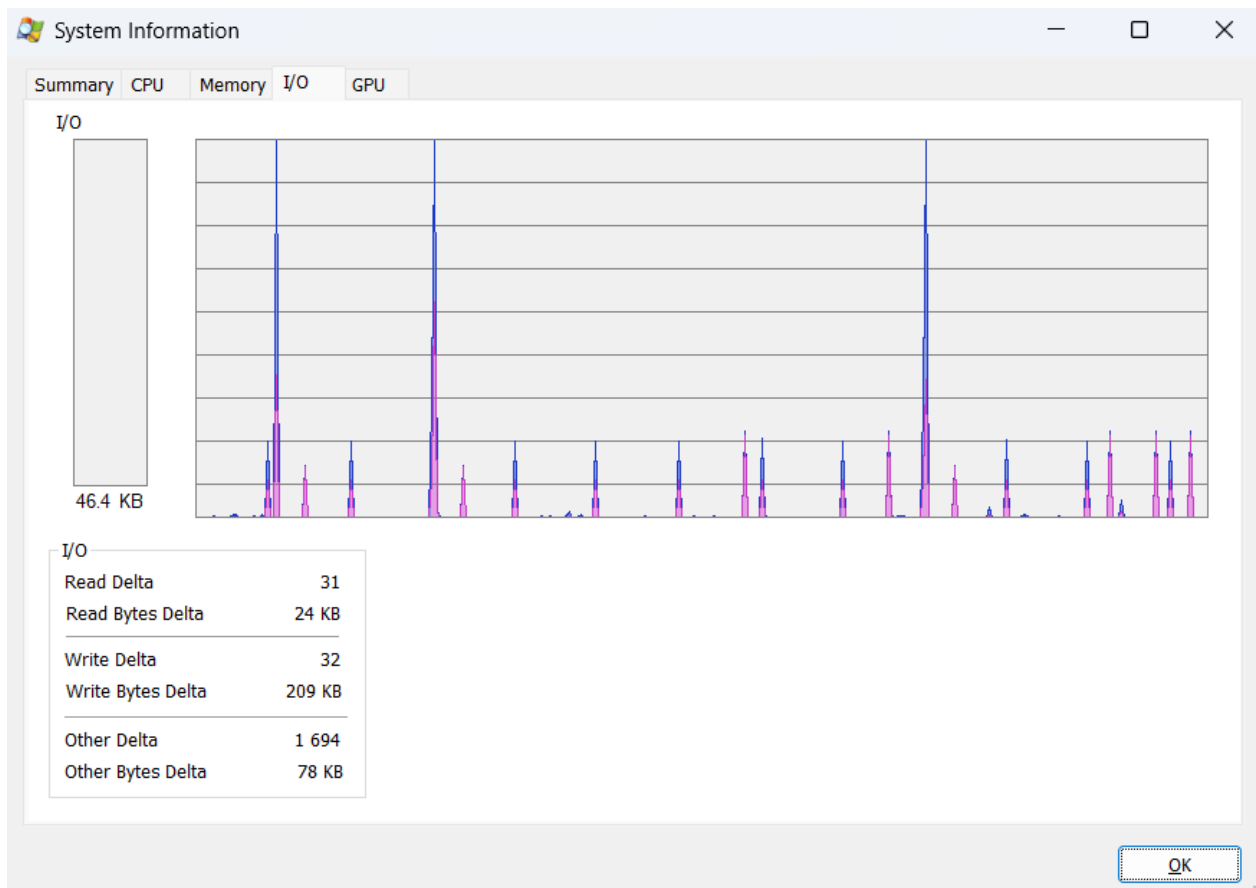


Рис. 9

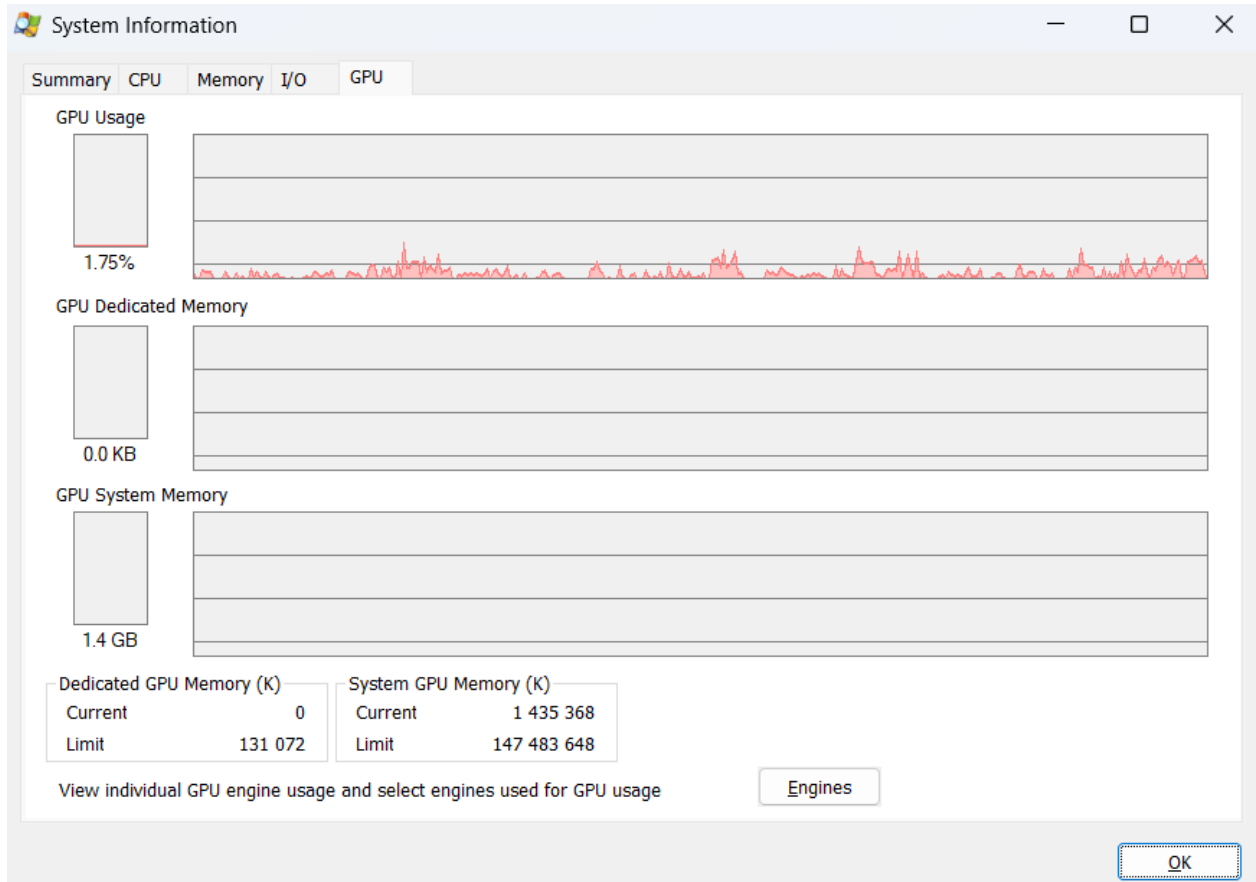


Рис. 10. Количество ядер процессора – 8, объём оперативной памяти компьютера – 10.4

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%

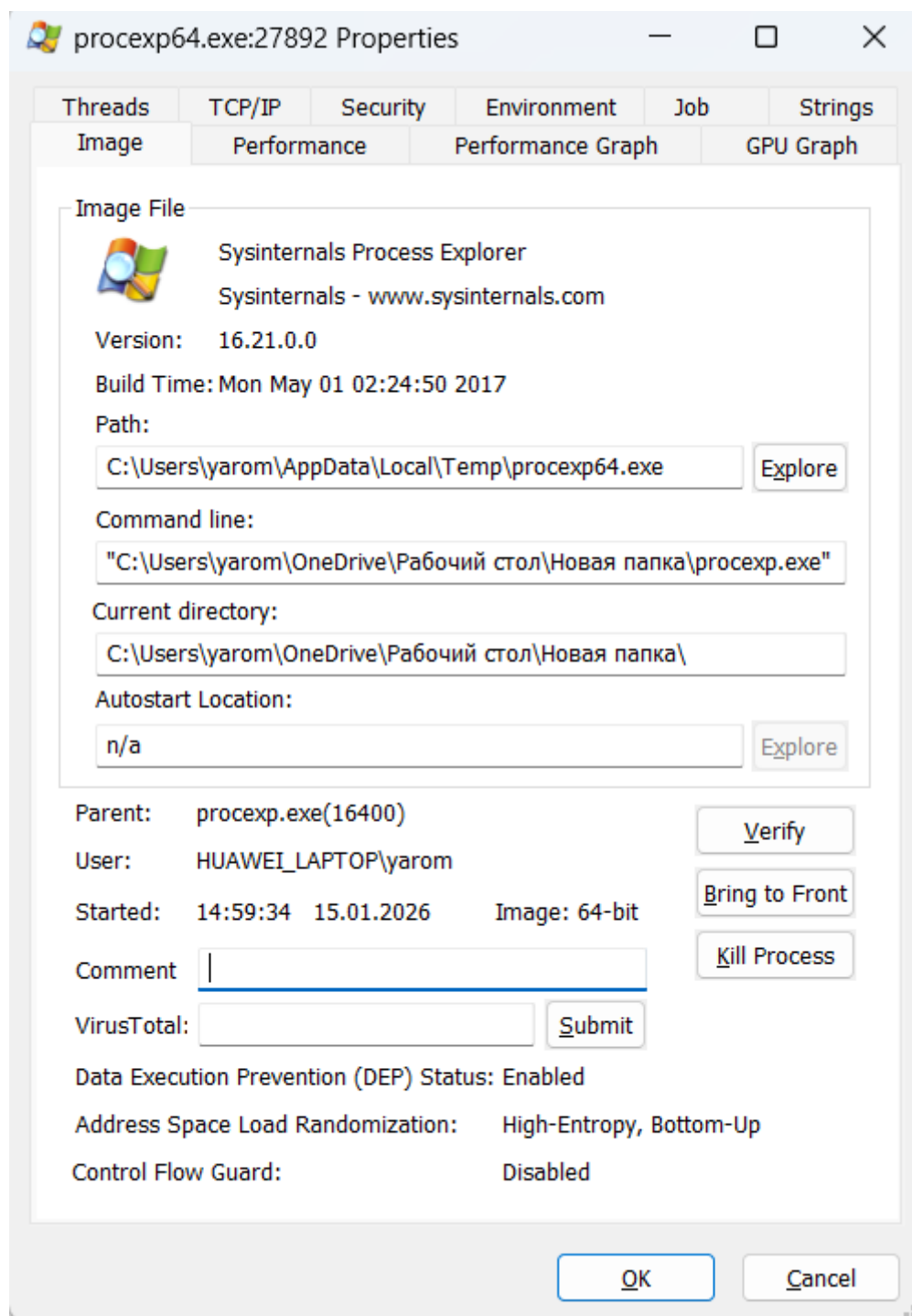


Рис. 11. Экранный снимок процесса

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

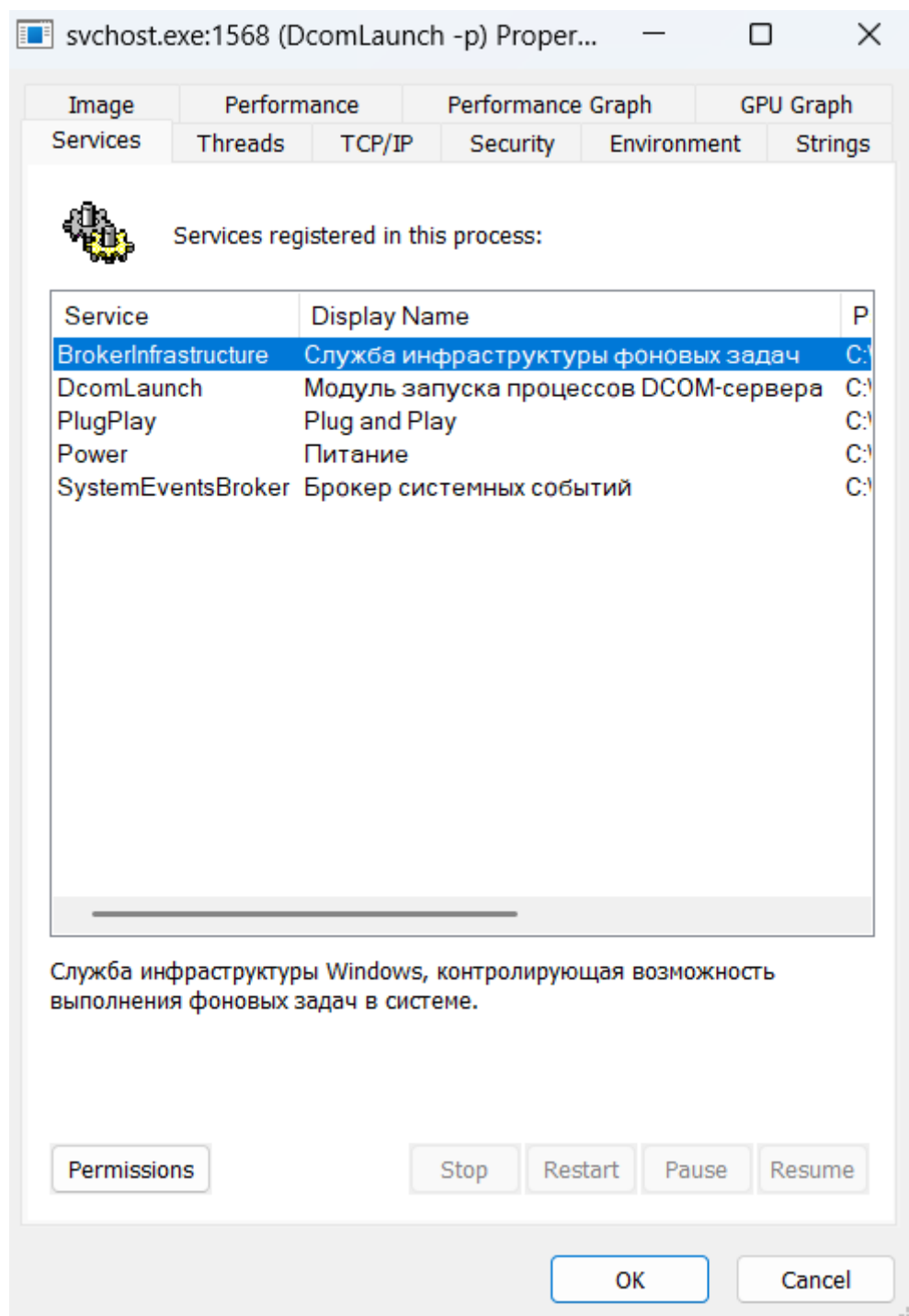


Рис. 12. Вкладка Services в процессе с наибольшим потреблением памяти svchost

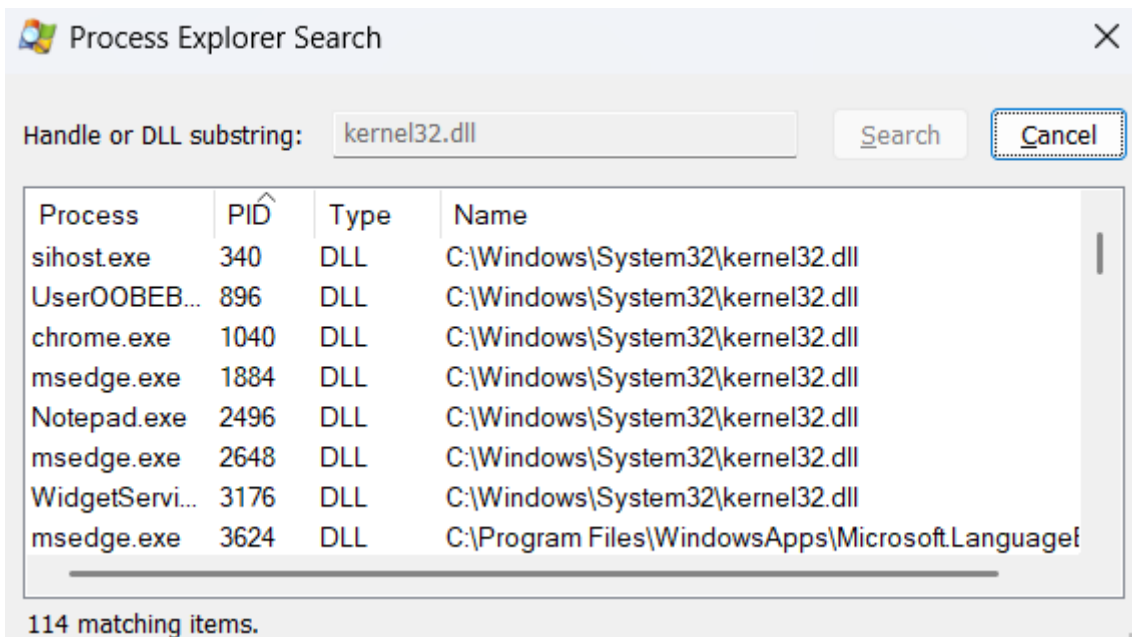


Рис. 13. Список процессов, использующих конкретную разделяемую библиотеку

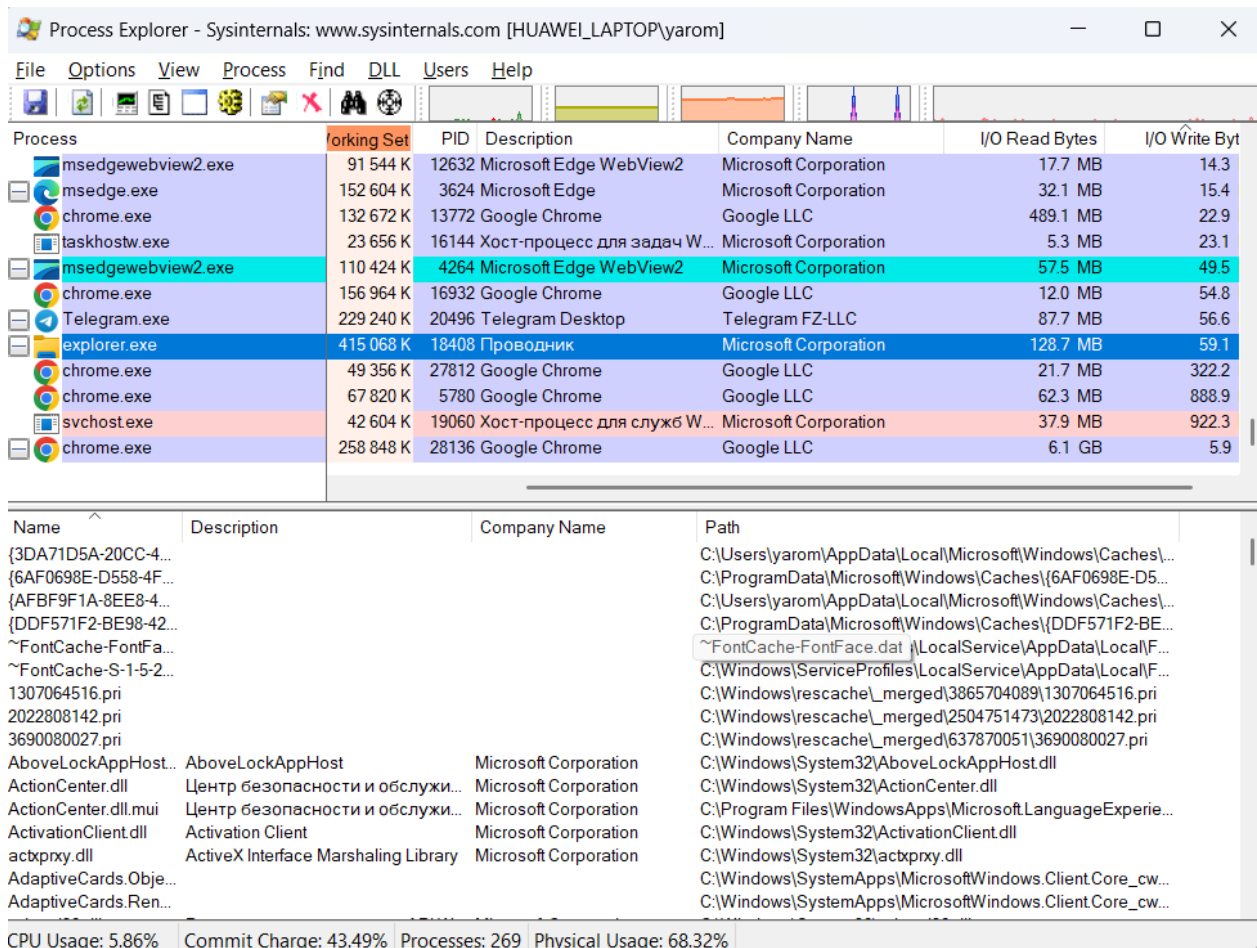


Рис. 14. Список разделяемых библиотек, используемых конкретным процессом

Диспетчер задач

Процессы

Производительность

Журнал приложений

Автозагрузка приложений

Пользователи

Сведения

Службы

Параметры

Процессы

Запустить новую задачу

...

| 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 бита) | | 0% | 0,3 МБ |
| > Adobe IPC Broker (32 бита) | | 0% | 1,0 МБ |
| > Antimalware Core Service | | 0% | 4,9 МБ |

Рис. 15

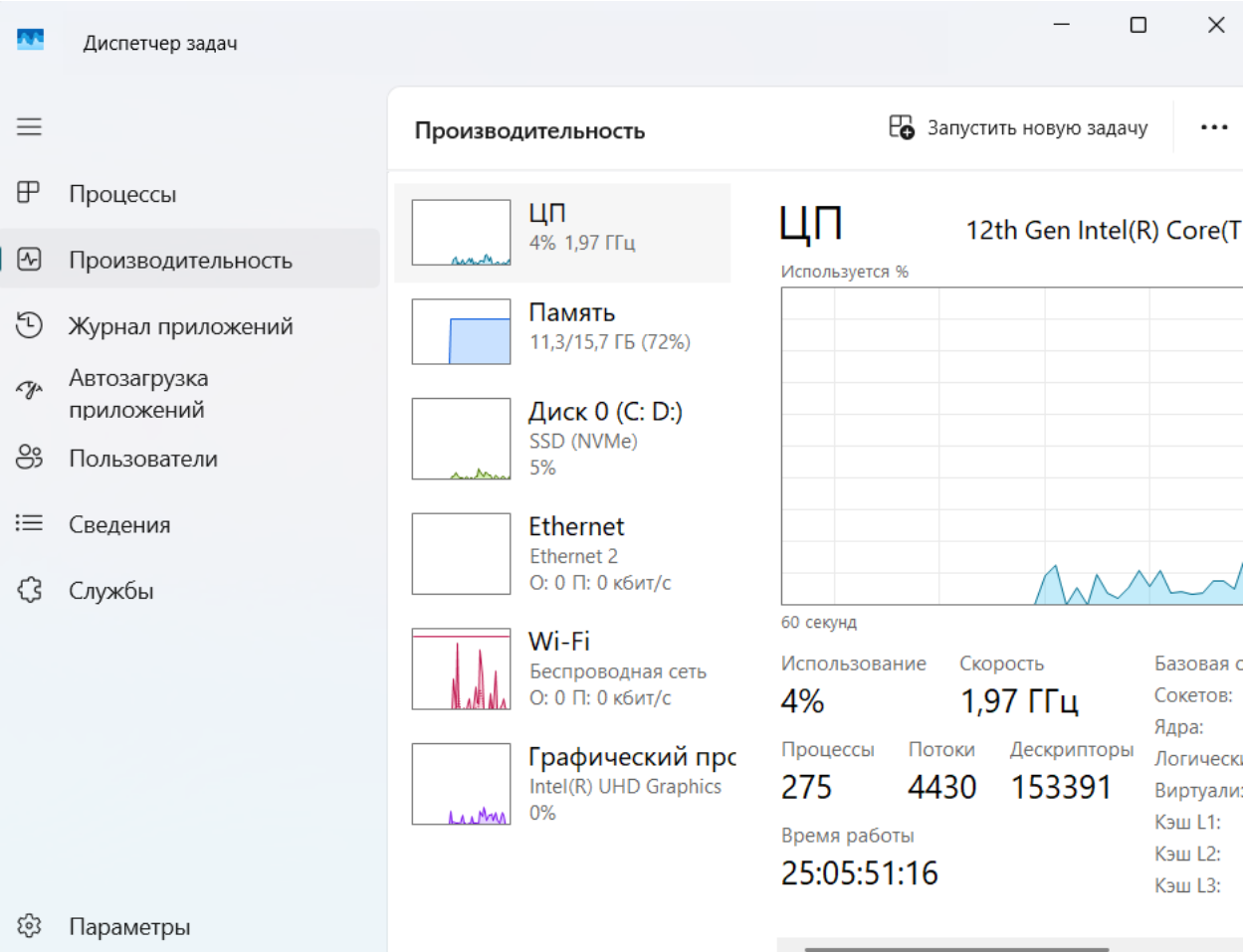


Рис. 16

Диспетчер задач

Процессы

Производительность

Журнал приложений

Автозагрузка приложений

Пользователи

Сведения

Службы

Параметры

Введите имя, издателя или PI...

Журнал приложений

Запустить новую задачу

Использование ресурсов с 16.12.2025 для учетных записей текущего пользователя и системы.
[Удалить журнал использования](#)

| Имя | Время ЦП | Сеть | Уведомления |
|--------------------|----------|------|-------------|
| Audio Console | 0:00:00 | 0 МБ | 0 МБ |
| audiodg | 0:00:01 | 0 МБ | 0 МБ |
| avp | 0:00:01 | 0 МБ | 0 МБ |
| avpui | 0:00:01 | 0 МБ | 0 МБ |
| bash | 0:00:01 | 0 МБ | 0 МБ |
| BasicService | 0:00:01 | 0 МБ | 0 МБ |
| CarambaSwitcher | 0:00:01 | 0 МБ | 0 МБ |
| chrome | 0:00:01 | 0 МБ | 0 МБ |
| conhost | 0:00:01 | 0 МБ | 0 МБ |
| csrss | 0:00:01 | 0 МБ | 0 МБ |
| ctfmon | 0:00:01 | 0 МБ | 0 МБ |
| Dev Home (Preview) | 0:00:00 | 0 МБ | 0 МБ |
| DFSSearchService | 0:00:01 | 0 МБ | 0 МБ |

Рис. 17

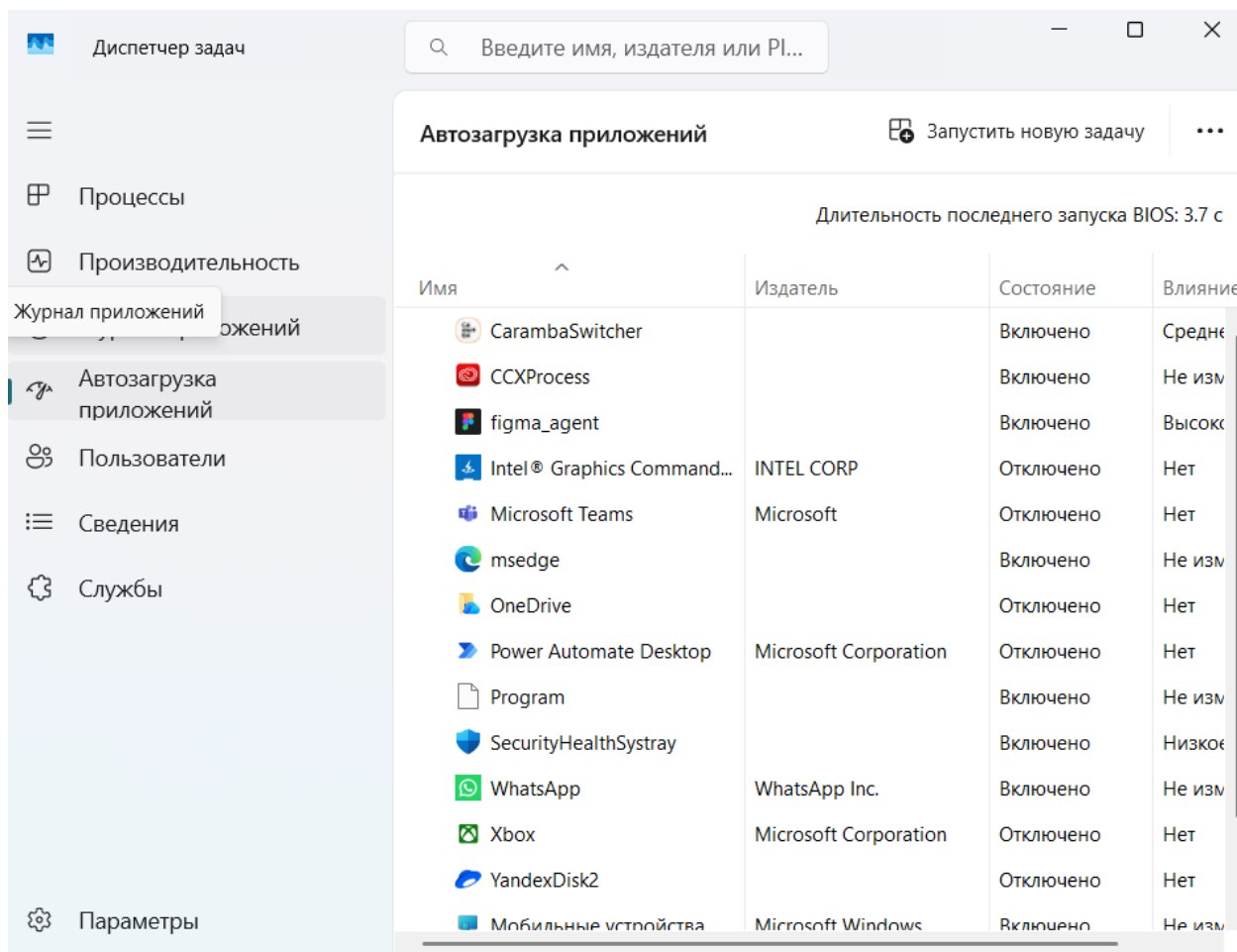


Рис. 18

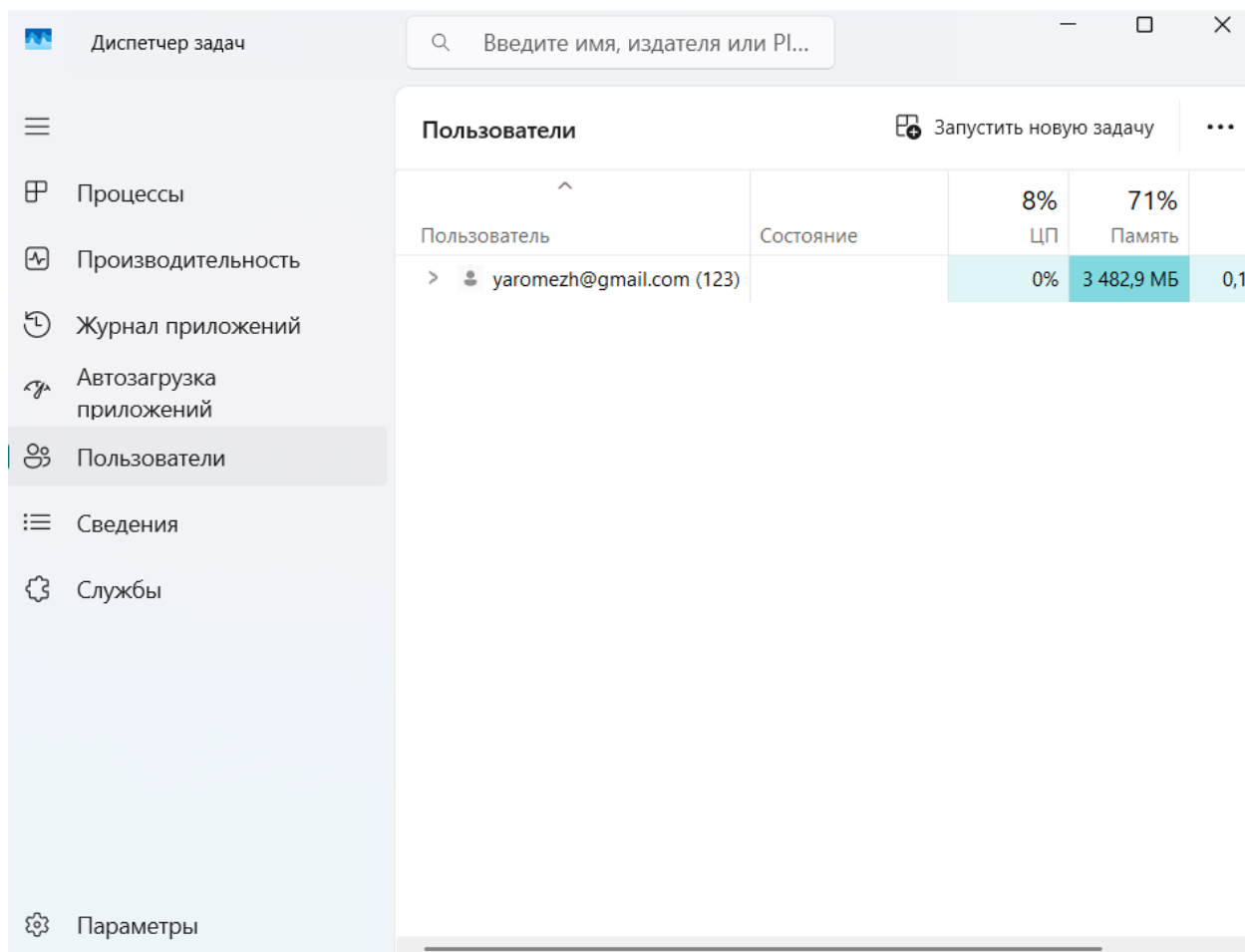


Рис. 19

Диспетчер задач

Процессы

Производительность

Журнал приложений

Автозагрузка приложений

Пользователи

Сведения

Службы

Параметры

Запустить новую задачу

...

Сведения

| Имя | ИД п... | Состо... | Имя польз... | ЦП | Дельт... | Платфо... | Вирту |
|-----------------------|---------|----------|--------------|----|----------|-----------|-------|
| AdobelPCBroker.exe | 23628 | Выпо... | yarom | 00 | 0 К | 32 бита | Откл. |
| AggregatorHost.exe | 8936 | Выпо... | СИСТЕМА | 00 | 0 К | 64 бита | Не р. |
| ApplicationFrameHo... | 16392 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| armsvc.exe | 4384 | Выпо... | СИСТЕМА | 00 | 0 К | 32 бита | Не р. |
| audiodg.exe | 19376 | Выпо... | LOCAL SER... | 00 | 0 К | 64 бита | Не р. |
| avp.exe | 4744 | Выпо... | СИСТЕМА | 00 | 0 К | 32 бита | Не р. |
| avp.exe | 8952 | Выпо... | СИСТЕМА | 00 | 0 К | 32 бита | Не р. |
| avpui.exe | 16688 | Выпо... | yarom | 00 | 0 К | 32 бита | Откл. |
| backgroundTaskHost... | 15700 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| bash.exe | 24676 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| BasicService.exe | 4632 | Выпо... | СИСТЕМА | 00 | 0 К | 64 бита | Не р. |
| CarambaSwitcher.exe | 6792 | Выпо... | yarom | 00 | 0 К | 32 бита | Откл. |
| CCXProcess.exe | 7720 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 28136 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 16580 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 13772 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 27812 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 22808 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 13076 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 18292 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 24624 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |
| chrome.exe | 9824 | Выпо... | yarom | 00 | 0 К | 64 бита | Откл. |

Рис. 20

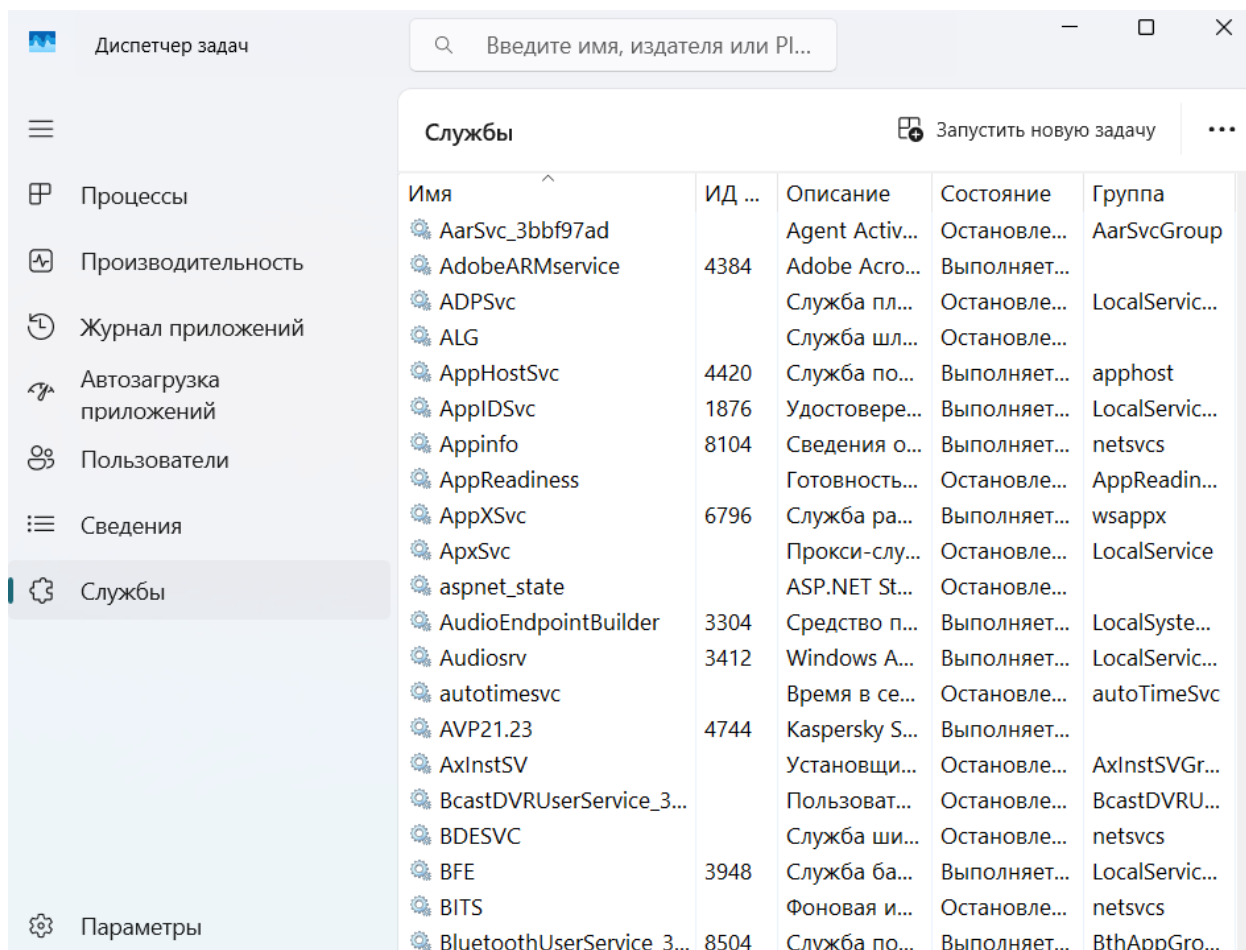


Рис. 21

| Autoruns - Sysinternals: www.sysinternals.com | | | | | |
|---|-----------------------------------|-----------------------|-----------------------------------|------------------|-------------|
| File Entry Options Help | | | | | |
| Filter: <input type="text"/> | | | | | |
| <div> <div>KnownDLLs</div> <div>Winlogon</div> <div>Winsock Providers</div> <div>Print Monitors</div> <div>LSA Providers</div> <div>Network Providers</div> <div>WMI</div> <div>Sidebar Gadgets</div> <div>Office</div> </div> <div> <div>Everything</div> <div>Login</div> <div>Explorer</div> <div>Internet Explorer</div> <div>Scheduled Tasks</div> <div>Services</div> <div>Drivers</div> <div>Codecs</div> <div>Boot Execute</div> <div>Image Hijacks</div> <div>AppInit</div> </div> | | | | | |
| Autorun Entry | Description | Publisher | Image Path | Timestamp | Virus Total |
| HKLM\System\CurrentControlSet\Services | | | | 15.01.2026 14:31 | |
| <input checked="" type="checkbox"/> AarSvc | Runtime for activating conver... | Microsoft Corporation | c:\windows\system32\aaarsvc... | 20.12.1987 3:02 | |
| <input checked="" type="checkbox"/> AarSvc_3bb97ad | Runtime for activating conver... | Microsoft Corporation | c:\windows\system32\svchost... | 21.06.1970 6:53 | |
| <input checked="" type="checkbox"/> AdobeARMServi... | Adobe Acrobat Updater keep... | Adobe Inc. | c:\program files (x86)\commo... | 25.08.2025 4:19 | |
| <input checked="" type="checkbox"/> ADPSvc | Эта служба используется ... | Microsoft Corporation | c:\windows\system32\adpsvc... | 18.04.1975 3:15 | |
| <input checked="" type="checkbox"/> ALG | Обеспечивает поддержку ... | Microsoft Corporation | c:\windows\system32\alg.exe | 03.05.2008 13:58 | |
| <input checked="" type="checkbox"/> AppHostSvc | Является административн... | Microsoft Corporation | c:\windows\system32\inetsrv\... | 06.03.2030 1:23 | |
| <input checked="" type="checkbox"/> AppIDSvc | Определяет и проверяет у... | Microsoft Corporation | c:\windows\system32\appids... | 19.05.1913 2:17 | |
| <input checked="" type="checkbox"/> Appinfo | Обеспечивает выполнени... | Microsoft Corporation | c:\windows\system32\appinfo... | 28.04.1957 1:57 | |
| <input checked="" type="checkbox"/> AppReadiness | Подготовка приложений к ... | Microsoft Corporation | c:\windows\system32\apprea... | 13.04.1954 10:46 | |
| <input checked="" type="checkbox"/> AppXSvc | Обеспечивает поддержку ... | Microsoft Corporation | c:\windows\system32\appxde... | 07.06.1905 1:18 | |
| <input checked="" type="checkbox"/> ApxSvc | Управляет виртуальными ... | Microsoft Corporation | c:\windows\system32\apxsvc... | 19.05.1956 6:02 | |
| <input checked="" type="checkbox"/> aspnet_state | Provides support for out-of-pr... | Microsoft Corporation | c:\windows\microsoft.net\fram... | 18.06.2025 23:26 | |
| <input checked="" type="checkbox"/> AudioEndpointBu... | Управление звуковыми ус... | Microsoft Corporation | c:\windows\system32\audioe... | 27.02.2025 8:47 | |
| <input checked="" type="checkbox"/> Audiosrv | Управление средствами р... | Microsoft Corporation | c:\windows\system32\audiosr... | 08.08.1936 6:42 | |
| <input checked="" type="checkbox"/> autotimesvc | Эта служба устанавливае... | Microsoft Corporation | c:\windows\system32\autotim... | 29.05.1974 6:25 | |
| <input checked="" type="checkbox"/> AVP21.23 | Обеспечивает защиту ком... | AO Kaspersky Lab | c:\program files (x86)\kaspers... | 10.06.2025 18:00 | |
| <input checked="" type="checkbox"/> AxInstSV | Обеспечивает проверку к... | Microsoft Corporation | c:\windows\system32\axinsts... | 22.01.1998 22:37 | |
| <input checked="" type="checkbox"/> BcastDVRUserSe... | Эта пользовательская слу... | Microsoft Corporation | c:\windows\system32\bcastd... | 26.01.2007 8:00 | |
| <input checked="" type="checkbox"/> BcastDVRUserSe... | Эта пользовательская слу... | Microsoft Corporation | c:\windows\system32\svchost... | 21.06.1970 6:53 | |
| <input checked="" type="checkbox"/> BDESVC | BDESVC предоставляет сл... | Microsoft Corporation | c:\windows\system32\bdesvc... | 16.04.2023 21:59 | |
| <input checked="" type="checkbox"/> BFE | Служба базовой фильтрац... | Microsoft Corporation | c:\windows\system32\bfe.dll | 11.10.1993 21:11 | |
| <input checked="" type="checkbox"/> BITS | Передаёт файлы в фоновом... | Microsoft Corporation | c:\windows\system32\qmgr.dll | 19.08.2035 23:39 | |
| <input checked="" type="checkbox"/> BluetoothUserSe... | Служба поддержки пользо... | Microsoft Corporation | c:\windows\system32\micros... | 02.02.1969 11:41 | |
| <input checked="" type="checkbox"/> BluetoothUserSe... | Служба поддержки пользо... | Microsoft Corporation | c:\windows\system32\svchost... | 21.06.1970 6:53 | |
| <input checked="" type="checkbox"/> BrokerInfrastructu... | Служба инфраструктуры ... | Microsoft Corporation | c:\windows\system32\psmsrv... | 23.01.2017 11:39 | |
| <input checked="" type="checkbox"/> BTAGService | Служба, поддерживающая ... | Microsoft Corporation | c:\windows\system32\btagserv... | 25.02.2019 9:05 | |
| <input checked="" type="checkbox"/> BthAvctnSvc | Эта служба протокола тра... | Microsoft Corporation | c:\windows\system32\bthavct... | 31.12.1938 20:57 | |
| Ready. | | | | | |
| No Filter. | | | | | |

Рис. 23. Вкладка **Scheduled Tasks**

Autoruns - Sysinternals: www.sysinternals.com

FileEntryOptionsHelp

Filter:

Everything

Login

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 | Virus Total |
|---|--|--|----------------------------------|------------------|-------------|
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers | | | | | |
| <input checked="" type="checkbox"/> | %windir%\system... "RdpCredentialProvider.DYN... | Microsoft Corporation | c:\windows\system32\rdpcred... | 11.06.1965 12:02 | |
| <input checked="" type="checkbox"/> | Automatic Redep... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\mgmtre... | 30.05.1997 18:59 | |
| <input checked="" type="checkbox"/> | CCertProvider | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\certcre... | 02.05.2007 13:16 | |
| <input checked="" type="checkbox"/> | Cloud Experienc... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\cxcred... | 28.03.1937 7:05 | |
| <input checked="" type="checkbox"/> | CngCredUICrede... | Поставщик Microsoft CNG Cr... Microsoft Corporation | c:\windows\system32\cngcre... | 18.03.1939 9:49 | |
| <input checked="" type="checkbox"/> | FaceCredentialPr... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\facecre... | 09.09.1918 23:53 | |
| <input checked="" type="checkbox"/> | FIDO Credential ... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\fidocre... | 25.02.1970 11:36 | |
| <input checked="" type="checkbox"/> | GenericProvider | Поставщики учетных данн... Microsoft Corporation | c:\windows\system32\credpro... | 22.12.1989 6:43 | |
| <input checked="" type="checkbox"/> | NGC Credential P... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\ngccre... | 09.12.1970 6:05 | |
| <input checked="" type="checkbox"/> | NPPProvider | Поставщики учетных данн... Microsoft Corporation | c:\windows\system32\credpro... | 22.12.1989 6:43 | |
| <input checked="" type="checkbox"/> | PasswordProvider | Поставщики учетных данн... Microsoft Corporation | c:\windows\system32\credpro... | 22.12.1989 6:43 | |
| <input checked="" type="checkbox"/> | PicturePassword... | Устаревшие поставщики у... Microsoft Corporation | c:\windows\system32\credpro... | 13.01.1997 14:01 | |
| <input checked="" type="checkbox"/> | PINLogonProvider | Устаревшие поставщики у... Microsoft Corporation | c:\windows\system32\credpro... | 13.01.1997 14:01 | |
| <input checked="" type="checkbox"/> | Second Authentic... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\device... | 04.12.1902 5:22 | |
| <input checked="" type="checkbox"/> | Smartcard Crede... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\smartc... | 04.12.2020 1:47 | |
| <input checked="" type="checkbox"/> | Smartcard Pin Pr... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\smartc... | 04.12.2020 1:47 | |
| <input checked="" type="checkbox"/> | Smartcard Read... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\smartc... | 04.12.2020 1:47 | |
| <input checked="" type="checkbox"/> | Smartcard WinR... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\smartc... | 04.12.2020 1:47 | |
| <input checked="" type="checkbox"/> | TrustedSignal Cr... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\trusteds... | 21.08.1985 14:57 | |
| <input checked="" type="checkbox"/> | WinBio Credentia... | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\biocred... | 12.07.1928 14:36 | |
| <input checked="" type="checkbox"/> | WLIDCredentialP... | Microsoft® Account Credential... Microsoft Corporation | c:\windows\system32\wldcre... | 16.04.1961 2:51 | |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters | | | | | |
| <input checked="" type="checkbox"/> | GenericFilter | Поставщики учетных данн... Microsoft Corporation | c:\windows\system32\credpro... | 22.12.1989 6:43 | |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers | | | | | |
| <input checked="" type="checkbox"/> | CRasProvider | Поставщик учетных данны... Microsoft Corporation | c:\windows\system32\rasplap... | 23.05.1922 9:17 | |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions | | | | | |
| <input checked="" type="checkbox"/> | {0ACDD40C-75A} | Клиент групповой политик... Microsoft Corporation | c:\windows\system32\wlgpclnt.dll | 08.1924 6:07 | |

Ready.

No Filter.

Рис. 24. Вставка Services

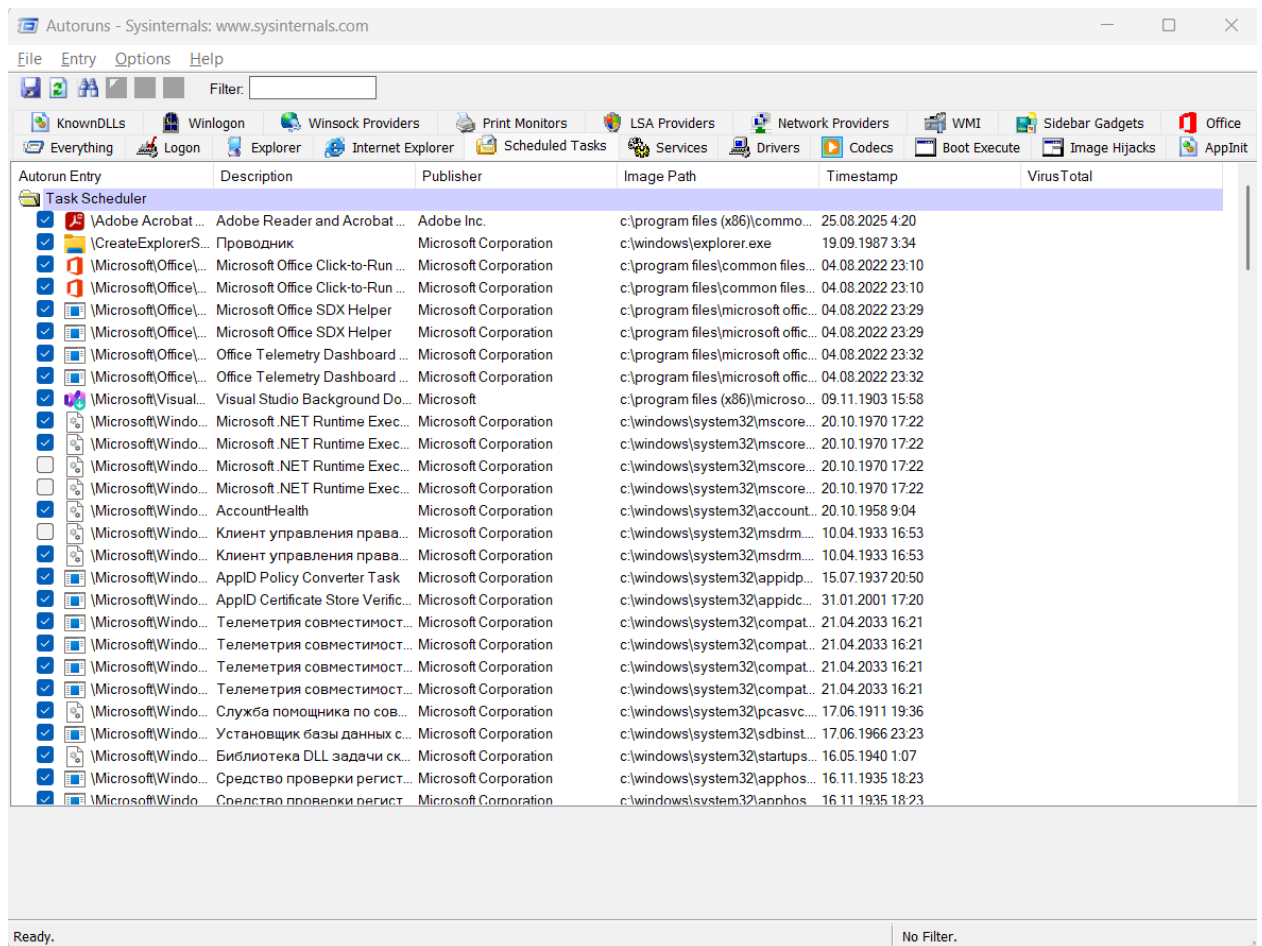


Рис. 25. Вставка Winlogon

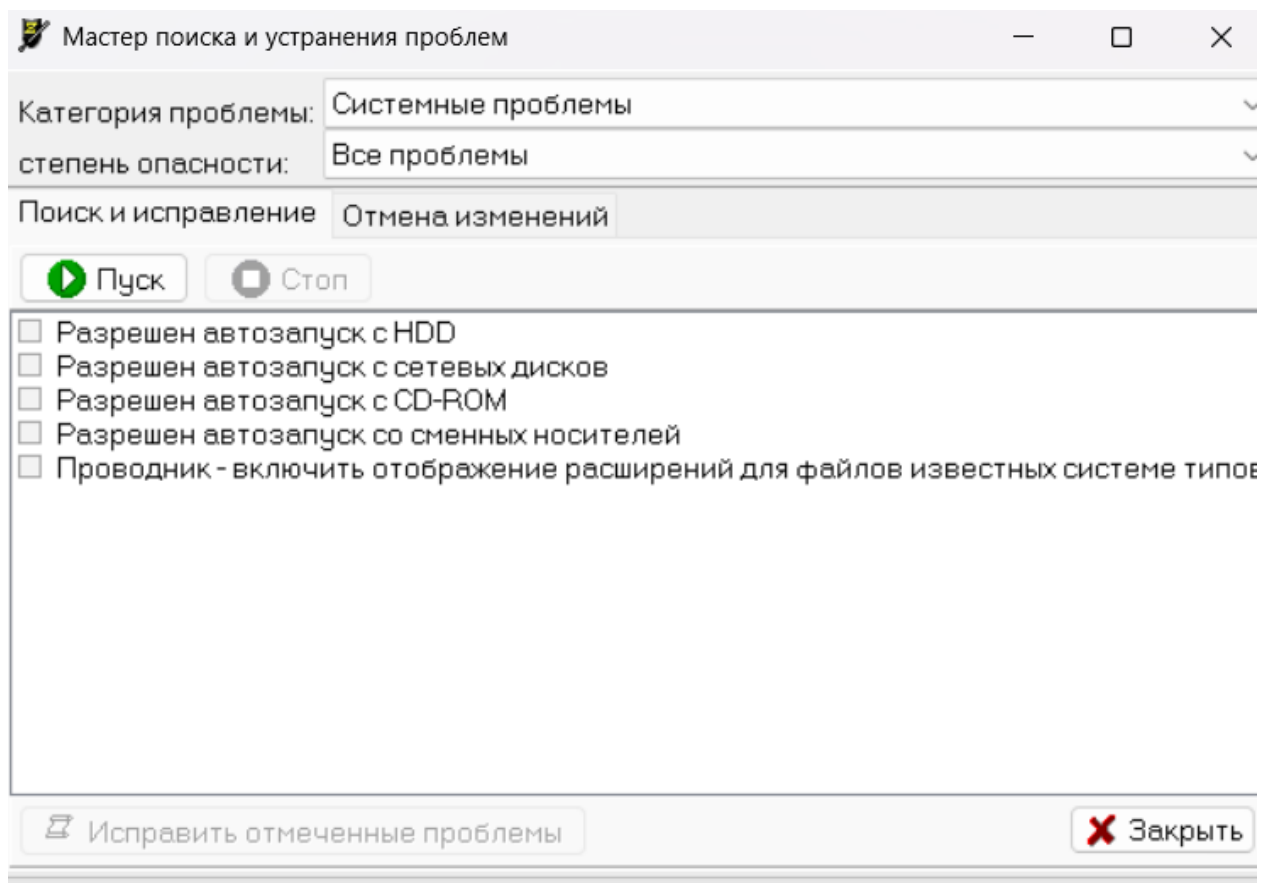


Рис. 26

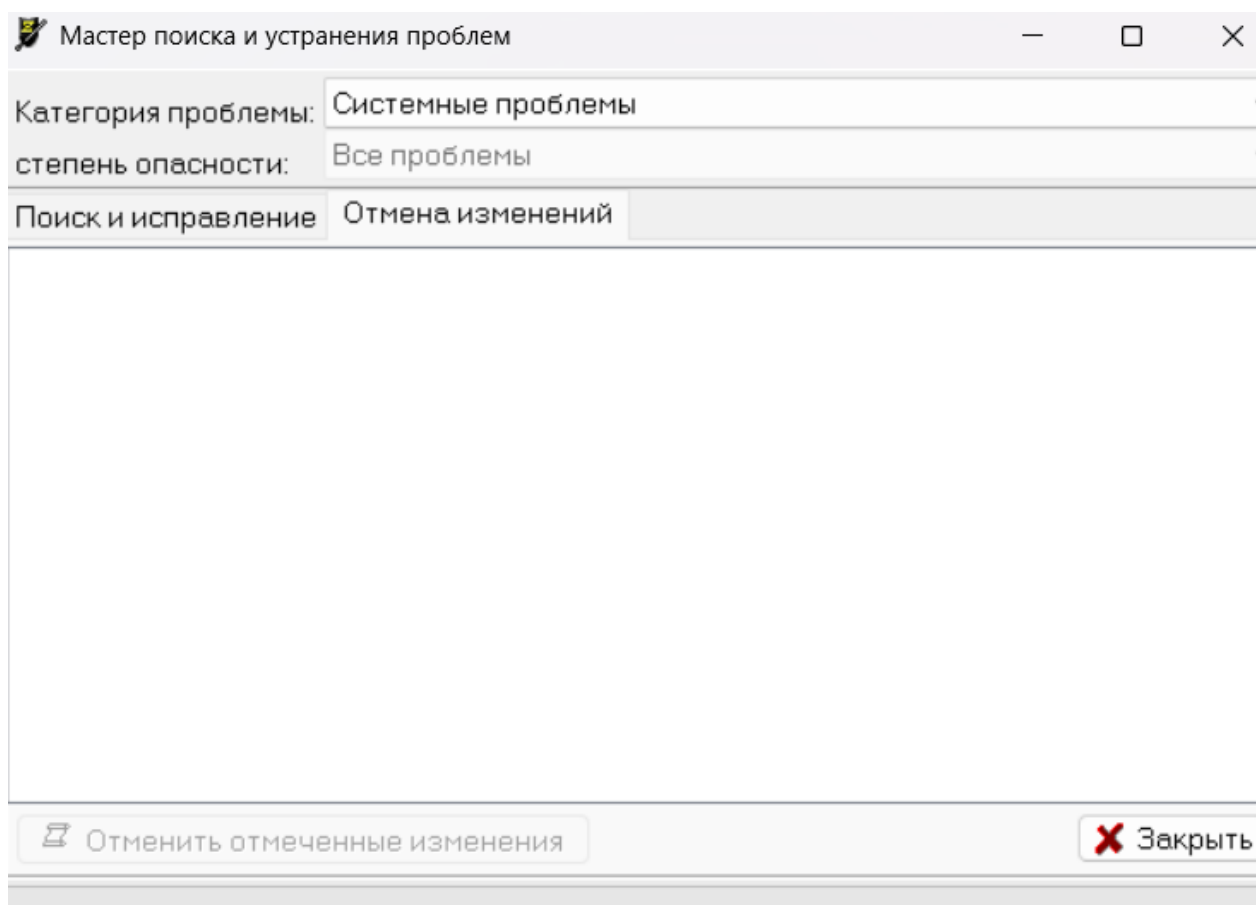


Рис. 27. Получите информацию об имеющихся в ОС проблемах


```
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 ->77C3948
```

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.