

**МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)**

**Институт №8 «Компьютерные науки и прикладная математика»
Кафедра 806 «Вычислительная математика и программирование»**

**Лабораторная работа №6
по курсу «Операционные системы»**

Выполнил: К. С. Шульц
Группа: М8О-208БВ-24
Преподаватель: Е. С. Миронов

Москва, 2025

Условие:

Цель работы:

Приобретение практических навыков диагностики работы программного обеспечения.

Задание:

При выполнении лабораторных работ по курсу ОС необходимо продемонстрировать ключевые системные вызовы, которые в них используются, проанализировать их.

Лабораторная работа №1: Анализ системных вызовов (Windows)

Программа: parent.exe

Цель: Создание двух дочерних процессов (child1.exe, child2.exe) и организация межпроцессного взаимодействия через каналы (pipes).

Ключевые системные вызовы

1. Создание дочерних процессов (аналог fork() + exec() в Linux)

```
"2:56:07,5591998","parent.exe","7664","Process Create",
"C:\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\child1.exe",
"SUCCESS","PID: 5316,Command line: child1.exe"
```

```
"2:56:09,7367104","parent.exe","7664","Process Create",
"C:\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\child2.exe",
"SUCCESS","PID: 2548,Command line: child2.exe"
```

Объяснение: Программа parent.exe создаёт два дочерних процесса child1.exe и child2.exe с помощью системного вызова Process Create (в Windows аналог CreateProcess), что соответствует fork() + exec() в Linux. Каждому процессу присваивается уникальный PID.

2. Открытие исполняемых файлов для запуска

```
"2:56:07,4526425","parent.exe","7664","CreateFile",
"C:\Users\kseni\...\\child1.exe","SUCCESS",...
```

```
"2:56:07,5661642","parent.exe","7664","CreateFile",
"C:\Users\kseni\...\\child2.exe","SUCCESS",...
```

Объяснение: Перед созданием процессов система проверяет доступность и права доступа к исполняемым файлам child1.exe и child2.exe через вызовы CreateFile.

3. Создание и работа с каналами (pipes)

(В логе не отображены явно, так как в Windows каналы создаются через CreatePipe() API, который внутри использует CreateFile для создания named pipe-объектов)

Объяснение: Для межпроцессного взаимодействия программа использует каналы (pipes). В Windows они создаются через CreatePipe(), который внутренне вызывает CreateFile для создания объектов типа pipe. Данные передаются через ReadFile/WriteFile.

4. Проверки совместимости и безопасности

```
"2:56:07,4545717", "parent.exe", "7664", "RegOpenKey",
"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options",
"SUCCESS", ...
```

```
"2:56:07,4546024", "parent.exe", "7664", "RegOpenKey",
"HKLM\SOFTWARE\...\Image File Execution Options\child1.exe",
"NAME NOT FOUND", ...
```

Объяснение: Windows проверяет реестр на наличие настроек совместимости и политик безопасности перед запуском исполняемых файлов.

5. Завершение работы

```
"2:57:04,0962884", "parent.exe", "7664", "Process Exit",
"", "SUCCESS", "Exit Status: 0, ..."
```

Объяснение: Программа корректно завершается с кодом 0. Все ресурсы (процессы, файловые дескрипторы) освобождаются.

Анализ работы программы на основе системных вызовов

Программа parent.exe демонстрирует классическую схему межпроцессного взаимодействия:

- Инициализация:** Загрузка необходимых DLL, проверка настроек системы и безопасности.
- Создание процессов:** Последовательный запуск двух независимых дочерних процессов child1.exe и child2.exe через Process Create.
- Организация IPC:** Создание каналов (pipes) для обмена данными между родительским и дочерними процессами.
- Выполнение логики:** Родительский процесс отправляет данные дочерним через каналы и получает результаты обработки.
- Корректное завершение:** Закрытие всех дескрипторов, завершение дочерних процессов и выход с кодом 0.

Вывод: Реализация соответствует требованиям лабораторной работы по созданию многопроцессных приложений с использованием IPC.

Лабораторная работа №2: Анализ системных вызовов (Windows)

Программа: median_filter.exe

Параметры запуска: -threads 4

Цель: Реализация медианного фильтра для обработки данных с использованием нескольких потоков (threads).

Ключевые системные вызовы

1. Запуск программы и инициализация

```
"3:12:22,5497293","median_filter.exe","22448","Process Start",
","","SUCCESS","Parent PID: 11604,Command line:
""C:\Users\kseni\lab2_OS_wind\lab2\build\median_filter.exe"" -threads 4,..."
```

Объяснение: Программа запускается с параметром -threads 4, что указывает на использование 4 потоков для параллельной обработки.

2. Создание потоков (threads)

```
"3:12:22,5498014","median_filter.exe","22448","Thread Create",
","","SUCCESS","Thread ID: 10252"
```

```
"3:12:47,2253625","median_filter.exe","22448","Thread Create",
","","SUCCESS","Thread ID: 20312"
```

```
"3:12:47,2253925","median_filter.exe","22448","Thread Create",
","","SUCCESS","Thread ID: 9128"
```

```
"3:12:47,2254221","median_filter.exe","22448","Thread Create",
","","SUCCESS","Thread ID: 8096"
```

```
"3:12:47,2254497","median_filter.exe","22448","Thread Create",
","","SUCCESS","Thread ID: 19576"
```

Объяснение: Создано 5 потоков:

- Thread ID 10252 — основной поток программы (создан при старте)
- Thread ID 20312, 9128, 8096, 19576 — рабочие потоки для параллельной обработки данных (соответствуют параметру -threads 4)

В Windows создание потока осуществляется через системный вызов Thread Create, который является аналогом pthread_create() в Linux.

3. Работа потоков и синхронизация

(В логе не отображены явные вызовы синхронизации типа CreateMutex, WaitForSingleObject, ReleaseMutex, так как ProcMon может не показывать внутренние синхронизационные вызовы ядра)

Объяснение: Для предотвращения гонок данных (race conditions) при доступе к общей переменной `nextRow` используется семафор с начальным значением 1 (бинарный семафор, эквивалентен мьютексу). Каждый поток перед чтением/изменением `nextRow` вызывает `wait()`, а после завершения работы с общей переменной — `signal()`.

4. Завершение потоков

```
"3:12:52,5606885","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 19996,..."
```

```
"3:13:17,2285648","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 9128,..."
```

```
"3:13:17,2286066","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 8096,..."
```

```
"3:13:17,2292343","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 19576,..."
```

```
"3:13:17,2293547","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 20312,..."
```

```
"3:13:17,2353137","median_filter.exe","22448","Thread Exit",
","","SUCCESS","Thread ID: 10252,..."
```

Объяснение: Все потоки корректно завершаются. Важно отметить:

- Рабочие потоки (20312, 9128, 8096, 19576) завершаются практически одновременно
- Основной поток (10252) завершается последним после ожидания завершения рабочих потоков
- Время выполнения: ~55 секунд (с 3:12:22 до 3:13:17)

5. Завершение процесса

```
"3:13:17,2358070","median_filter.exe","22448","Process Exit",
","","SUCCESS","Exit Status: 0,..."
```

Объяснение: Процесс завершается с кодом 0 (успешно). Все ресурсы (память, дескрипторы) освобождаются.

Анализ работы программы на основе системных вызовов

Программа `median_filter.exe` демонстрирует классическую архитектуру многопоточного приложения:

1. **Инициализация:** Загрузка программы, проверка системных настроек, создание основного потока.

2. **Создание рабочих потоков:** В соответствии с параметром `-threads 4` создаются 4 рабочих потока для параллельной обработки данных.
3. **Распределение работы:** Исходные данные разделяются между потоками для одновременной обработки.
4. **Синхронизация:** Используются механизмы синхронизации для:
 - Безопасного доступа к общим данным
 - Координации работы потоков
 - Сбора результатов
5. **Завершение:** Рабочие потоки завершаются после выполнения задач, основной поток собирает результаты и завершает программу.

Особенности реализации для медианного фильтра

- **Параллельная обработка изображения/данных:** Каждый поток обрабатывает свой сегмент данных.
- **Масштабируемость:** Программа может использовать разное количество потоков в зависимости от параметра `-threads`.

Вывод: Реализация соответствует требованиям лабораторной работы по созданию многопоточных приложений с возможностью настройки количества потоков выполнения и с их синхронизацией.

Лабораторная работа №3: Анализ системных вызовов (Windows)

Программа: parent.exe

Цель: Создание двух дочерних процессов (child1.exe, child2.exe) и организация межпроцессного взаимодействия через Memory-Mapped Files (MMF).

Ключевые системные вызовы

1. Создание дочерних процессов

```
"23:43:40,6734533", "parent.exe", "20288", "Process Create",
"C:\Users\kseni\lab30SWaL\lab30S\build\bin\child1.exe",
"SUCCESS", "PID: 20304,Command line: child1.exe parent_to_child1 child1_to_child2"

"23:43:40,6901308", "parent.exe", "20288", "Process Create",
"C:\Users\kseni\lab30SWaL\lab30S\build\bin\child2.exe",
"SUCCESS", "PID: 20140,Command line: child2.exe child1_to_child2 child2_to_parent"
```

Объяснение: Программа parent.exe создаёт два дочерних процесса child1.exe и child2.exe с помощью системного вызова Process Create. В командной строке передаются имена объектов MMF для межпроцессного взаимодействия.

2. Подготовка исполняемых файлов через Memory-Mapped Files

```
"23:43:40,6708468","parent.exe","20288","CreateFileMapping",
"C:\Users\kseni\lab30SWaL\lab30S\build\bin\child1.exe",
"SUCCESS","SyncType: SyncType0ther"
```

```
"23:43:40,6747189","parent.exe","20288","CreateFileMapping",
"C:\Users\kseni\lab30SWaL\lab30S\build\bin\child1.exe",
"SUCCESS","SyncType: SyncType0ther"
```

```
"23:43:40,6932166","parent.exe","20288","CreateFileMapping",
"C:\Users\kseni\lab30SWaL\lab30S\build\bin\child2.exe",
"SUCCESS","SyncType: SyncType0ther"
```

Объяснение: Перед запуском процессов система создаёт memory-mapped файлы для исполняемых модулей через CreateFileMapping. Это позволяет эффективно загружать код в память и разделять его между процессами.

3. Работа с системными базами данных совместимости

```
"23:43:40,6624485","parent.exe","20288","CreateFileMapping",
"C:\Windows\apppatch\sysmain.sdb","SUCCESS","SyncType: SyncType0ther"
```

```
"23:43:40,6628833","parent.exe","20288","CreateFileMapping",
"C:\Windows\apppatch\MergeSdbFilesSource\sysMerge.sdb",
"SUCCESS","SyncType: SyncType0ther"
```

Объяснение: Windows использует memory-mapped файлы для загрузки баз данных совместимости приложений (sysmain.sdb, sysMerge.sdb), что ускоряет проверку настроек совместимости.

4. Проверки безопасности и совместимости через реестр

```
"23:43:40,6599471","parent.exe","20288","RegOpenKey",
"HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers",
"SUCCESS","Desired Access: Query Value"
```

```
"23:43:40,6707088","parent.exe","20288","RegOpenKey",
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\child
"NAME NOT FOUND","Desired Access: Query Value,Enumerate Sub Keys"
```

Объяснение: Система проверяет политики безопасности (Safer) и настройки совместимости (Image File Execution Options) перед запуском процессов.

5. Завершение работы процессов

```
"23:44:24,5532847","parent.exe","20288","Process Exit",
","","SUCCESS","Exit Status: 0,User Time: 0.0000000 seconds,..."
```

Объяснение: Родительский процесс корректно завершается с кодом 0. Все ресурсы (процессы, MMF, дескрипторы) освобождаются.

Анализ работы программы на основе системных вызовов

Программа parent.exe демонстрирует организацию межпроцессного взаимодействия через Memory-Mapped Files:

1. **Инициализация:** Загрузка системных DLL, проверка настроек реестра, подготовка MMF для исполняемых файлов.
2. **Создание процессов с передачей имён MMF:** Дочерние процессы получают через командную строку имена объектов Memory-Mapped Files для организации цепочки обмена данными: parent_to_child1, child1_to_child2, child2_to_parent.
3. **Использование MMF вместо pipes:** В отличие от 1 лабораторной работы, где использовались pipes, здесь межпроцессное взаимодействие организовано через memory-mapped files. Это позволяет:
 - Осуществлять более быстрый обмен большими объёмами данных
 - Разделять память между процессами
 - Упрощать синхронизацию через файловые отображения
4. **Проверка безопасности:** Система выполняет проверки через AppCompatFlags, Safer CodeIdentifiers, Image File Execution Options для обеспечения безопасного выполнения.
5. **Оптимизация через MMF:** Исполняемые файлы и системные базы данных загружаются через CreateFileMapping, что уменьшает время загрузки и экономит память за счёт разделения кода между процессами.
6. **Корректное завершение:** Все MMF закрываются, процессы завершаются в правильном порядке.

Вывод: Реализация соответствует требованиям лабораторной работы по созданию многопроцессных приложений с использованием Memory-Mapped Files для межпроцессного взаимодействия. Программа демонстрирует эффективное использование системных механизмов Windows для организации IPC с улучшенной производительностью по сравнению с pipe-based решением.

Лабораторная работа №4: Анализ системных вызовов (Windows)

Программы: Program1.exe (статическая линковка), Program2.exe (динамическая линковка)

Цель: Сравнение механизмов статической и динамической линковки библиотек на примере двух программ, использующих библиотеки lib1.dll и lib2.dll с различными реализациями алгоритмов вычисления числа Пи и сортировки массивов.

Ключевые системные вызовы

1. Статическая линковка (Program1.exe)

```
"17:09:14,7611324","Program1.exe","20912","CreateFile",
"C:\Users\kseni\lab4_OS\build\liblib1.dll",
"SUCCESS","Desired Access: Read Attributes,..."  
  
"17:09:14,7614141","Program1.exe","20912","CreateFileMapping",
"C:\Users\kseni\lab4_OS\build\liblib1.dll",
"SUCCESS","SyncType: SyncType0ther"  
  
"17:09:14,7615829","Program1.exe","20912","Load Image",
"C:\Users\kseni\lab4_OS\build\liblib1.dll",
"SUCCESS","Image Base: 0x7ffcebd80000,Image Size: 0xc8000"
```

Объяснение: Программа Program1.exe использует статическую линковку. Системные вызовы CreateFile и CreateFileMapping показывают, что библиотека lib1.dll загружается как единое целое с исполняемым файлом на этапе запуска. Библиотека отображается в память процесса с фиксированным базовым адресом (0x7ffcebd80000).

2. Динамическая линковка (Program2.exe) - множественная загрузка

```
"17:11:00,9537398","Program2.exe","8972","Load Image",
"C:\Users\kseni\lab4_OS\build\lib1.dll",
"SUCCESS","Image Base: 0x7ffca2580000,Image Size: 0xc8000"  
  
"17:11:06,3641161","Program2.exe","8972","Load Image",
"C:\Users\kseni\lab4_OS\build\lib2.dll",
"SUCCESS","Image Base: 0x7ffca2580000,Image Size: 0xc8000"  
  
"17:11:10,2542536","Program2.exe","8972","Load Image",
"C:\Users\kseni\lab4_OS\build\lib1.dll",
"SUCCESS","Image Base: 0x7ffca2580000,Image Size: 0xc8000"
```

Объяснение: Программа Program2.exe демонстрирует динамическую загрузку библиотек. Библиотеки lib1.dll и lib2.dll загружаются в процессе выполнения программы. Обе библиотеки загружаются по одному базовому адресу (0x7ffca2580000) - говорит о механизме перезаписи библиотек в памяти при динамической загрузке.

3. Использование Memory-Mapped Files для загрузки DLL

```
"17:11:00,9535635","Program2.exe","8972","CreateFileMapping",
"C:\Users\kseni\lab4_OS\build\lib1.dll",
"SUCCESS","SyncType: SyncType0ther"  
  
"17:11:06,3638855","Program2.exe","8972","CreateFileMapping",
"C:\Users\kseni\lab4_OS\build\lib2.dll",
"SUCCESS","SyncType: SyncType0ther"
```

Объяснение: Windows использует механизм Memory-Mapped Files для загрузки динамических библиотек. Системный вызов CreateFileMapping создаёт отображение DLL-файла в память процесса, что позволяет эффективно загружать и разделять код библиотек между процессами.

4. Проверка политик безопасности

```
"17:09:14,7604002","Program1.exe","20912","RegOpenKey",
"HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers",
"SUCCESS","Desired Access: Query Value"
```

```
"17:11:00,9518573","Program2.exe","8972","RegOpenKey",
"HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers",
"SUCCESS","Desired Access: Query Value"
```

5. Проверка правил безопасности программ (SRP)

```
"17:09:14,7614884","Program1.exe","20912","RegQueryValue",
"HKLM\System\CurrentControlSet\Control\Srp\Gp\RuleCount",
"SUCCESS","Type: REG_DWORD,Length: 4,Data: 2"
```

```
"17:11:00,9536380","Program2.exe","8972","RegQueryValue",
"HKLM\System\CurrentControlSet\Control\Srp\Gp\RuleCount",
"SUCCESS","Type: REG_DWORD,Length: 4,Data: 2"
```

6. Завершение работы программ

```
"17:09:34,8707727","Program1.exe","20912","Process Exit",
","", "SUCCESS", "Exit Status: 0,..."
```

```
"17:11:24,0992375","Program2.exe","8972","Process Exit",
","", "SUCCESS", "Exit Status: 0,..."
```

Объяснение: Обе программы корректно завершаются с кодом 0. Все ресурсы (загруженные библиотеки, файловые дескрипторы, memory-mapped файлы) освобождаются системой.

Анализ различий в работе программ

1. Время работы и загрузки библиотек

- **Program1 (статическая):** Библиотека загружается один раз при запуске (17:09:14). Общее время работы: 20 секунд.
- **Program2 (динамическая):** Библиотеки загружаются многоократно в процессе выполнения (17:11:00, 17:11:06, 17:11:10). Общее время работы: 23 секунды.

2. Переключение библиотек Program2

Program1 (статическая):

17:09:14 -Загрузка liblib1.dll (однократно)

Program2 (динамическая):

17:11:00 -Загрузка lib1.dll

17:11:06 -Загрузка lib2.dll (замещает lib1.dll)

17:11:10 -Повторная загрузка lib1.dll (замещает lib2.dll)

Объяснение: библиотеки подгружаются и выгружаются динамически, позволяя переключаться между различными реализациями алгоритмов вычисления числа Пи и сортировки во время выполнения.

Выводы

- Статическая линковка (Program1)** обеспечивает более простую модель развертывания - все зависимости включены в исполняемый файл. Однако она не позволяет изменять реализацию алгоритмов без перекомпиляции всей программы.
- Динамическая линковка (Program2)** предоставляет гибкость - возможность замены алгоритмов во время выполнения программы.
- Системные вызовы Windows** для работы с DLL включают: CreateFile, CreateFileMapping, Load Image для загрузки; проверку политик безопасности через реестр; использование механизма Memory-Mapped Files для эффективной загрузки кода.

Результаты:

Общие выводы по анализу системных вызовов Windows

На основе анализа системных вызовов в 4 лабораторных работах можно сделать следующие выводы:

1. Windows использует единый подход к управлению процессами.

Все программы проходят одинаковые этапы запуска: создание процесса, загрузка системных библиотек (ntdll.dll, kernel32.dll), проверка настроек безопасности через реестр.

2. Безопасность — приоритет.

Перед выполнением любого кода Windows выполняет многоуровневые проверки: проверяет политики безопасности (Safer CodeIdentifiers), настройки совместимости (Image File Execution Options) и правила ограничения программ (Software Restriction Policies).

3. Memory-Mapped Files — универсальный механизм.

Windows использует один и тот же механизм (CreateFileMapping) для разных задач: загрузки исполняемых файлов, разделения данных между процессами и работы с системными базами данных.

4. Архитектура развивается от простого к сложному.

Лабораторные работы показывают эволюцию: от простых пайпов для обмена данными, к эффективным Memory-Mapped Files, и далее к динамической загрузке библиотек для максимальной гибкости.

Системные вызовы:

1 Лабораторная работа.

```
"2:56:07,4218780","parent.exe","7664","Process Start","","SUCCESS","Parent  
PID: 20876,Command line: ""C:\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\p  
"2:56:07,4218908","parent.exe","7664","Thread Create","","SUCCESS","Thread  
ID: 1932"  
"2:56:07,4503098","parent.exe","7664","Thread Create","","SUCCESS","Thread  
ID: 4396"  
"2:56:07,4536739","parent.exe","7664","Thread Create","","SUCCESS","Thread  
ID: 15508"  
"2:56:07,4367024","parent.exe","7664","Load Image","C:\Users\kseni\lab10S\lab10SLinux  
Base: 0x7ff78eb90000,Image Size: 0xd8e000"  
"2:56:07,4367872","parent.exe","7664","Load Image","C:\Windows\System32\ntdll.dll","S  
Base: 0x7ff8151b0000,Image Size: 0x217000"  
"2:56:07,4391048","parent.exe","7664","Load Image","C:\Windows\System32\kernel32.dll"  
Base: 0x7ff8146b0000,Image Size: 0xc4000"  
"2:56:07,4393972","parent.exe","7664","Load Image","C:\Windows\System32\KernelBase.dl  
Base: 0x7ff812940000,Image Size: 0x3b7000"  
"2:56:07,4501641","parent.exe","7664","Load Image","C:\Windows\System32\msvcrt.dll","  
Base: 0x7ff8149e0000,Image Size: 0xa7000"  
"2:56:07,4532153","parent.exe","7664","Load Image","C:\Windows\System32\sechost.dll",  
Base: 0x7ff814480000,Image Size: 0xa8000"  
"2:56:07,4535080","parent.exe","7664","Load Image","C:\Windows\System32\bcrypt.dll",  
Base: 0x7ff812560000,Image Size: 0x28000"  
"2:56:07,5591998","parent.exe","7664","Process Create","C:\Users\kseni\lab10S\lab10SL  
5316,Command line: child1.exe"  
"2:56:09,7367104","parent.exe","7664","Process Create","C:\Users\kseni\lab10S\lab10SL  
2548,Command line: child2.exe"  
"2:56:07,4526425","parent.exe","7664","CreateFile","C:\Users\kseni\lab10S\lab10SLinux"  
Access: Read Attributes..."  
"2:56:07,4547598","parent.exe","7664","CreateFile","C:\Users\kseni\lab10S\lab10SLinux"  
Access: Read Data/List Directory..."  
"2:56:07,5661642","parent.exe","7664","CreateFile","C:\Users\kseni\lab10S\lab10SLinux"  
Access: Read Attributes..."  
"2:56:07,5666639","parent.exe","7664","CreateFile","C:\Users\kseni\lab10S\lab10SLinux"  
Access: Read Data/List Directory..."  
"2:56:07,5539766","parent.exe","7664","CreateFileMapping","C:\Users\kseni\lab10S\lab1  
SyncTypeOther"  
"2:56:09,7322628","parent.exe","7664","CreateFileMapping","C:\Users\kseni\lab10S\lab1  
SyncTypeOther"  
"2:56:07,4373024","parent.exe","7664","RegOpenKey","HKLM\System\CurrentControlSet\Con  
Access: Read"  
"2:56:07,4545717","parent.exe","7664","RegOpenKey","HKLM\Software\Microsoft\Windows  
NT\CurrentVersion\Image File Execution Options","SUCCESS","Desired Access:  
Query Value,Enumerate Sub Keys"  
"2:56:07,4546024","parent.exe","7664","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Image File Execution Options\child1.exe","NAME NOT FOUND","Desired
```

```
Access: Query Value,Enumerate Sub Keys"
"2:56:07,5665589","parent.exe","7664","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired
Access: Query Value,Enumerate Sub Keys"
"2:56:07,4456408","parent.exe","7664","QuerySecurityFile","C:\Users\kseni\lab10S\lab1
Owner"
"2:56:07,5540526","parent.exe","7664","QuerySecurityFile","C:\Users\kseni\lab10S\lab1
Label"
"2:56:09,7323516","parent.exe","7664","QuerySecurityFile","C:\Users\kseni\lab10S\lab1
Label"
"2:56:07,4515076","parent.exe","7664","QueryNameInformationFile","C:\Users\kseni\lab1
\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\parent.exe"
"2:56:07,5541022","parent.exe","7664","QueryNameInformationFile","C:\Users\kseni\lab1
\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\child1.exe"
"2:56:09,7324092","parent.exe","7664","QueryNameInformationFile","C:\Users\kseni\lab1
\Users\kseni\lab10S\lab10SLinuxToWind\lab10S\build\bin\child2.exe"
"2:56:37,4641806","parent.exe","7664","Thread Exit","","SUCCESS","Thread ID:
4396,User Time: 0.0000000,Kernel Time: 0.0000000"
"2:56:37,4643027","parent.exe","7664","Thread Exit","","SUCCESS","Thread ID:
15508,User Time: 0.0000000,Kernel Time: 0.0000000"
"2:57:04,0958748","parent.exe","7664","Thread Exit","","SUCCESS","Thread ID:
1932,User Time: 0.0156250,Kernel Time: 0.0468750"
"2:57:04,0962884","parent.exe","7664","Process Exit","","SUCCESS","Exit Status:
0,User Time: 0.0156250 seconds,Kernel Time: 0.0468750 seconds,Private Bytes:
802 816,Peak Private Bytes: 905 216,Working Set: 18 182 144,Peak Working Set:
18 231 296"
```

2 Лабораторная работа.

```
"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"3:12:22,5497293","median_filter.exe","22448","Process Start","","SUCCESS","Parent
PID: 11604,Command line: ""C:\Users\kseni\lab2_OS_wind\lab2\build\median_filter.exe"""
-threads 4"
"3:12:22,5498014","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 10252"
"3:12:22,5549134","median_filter.exe","22448","Load Image","C:\Users\kseni\lab2_OS_wi
Base: 0x7ff767910000,Image Size: 0xd7a000"
"3:12:22,5550913","median_filter.exe","22448","Load Image","C:\Windows\System32\ntdll
Base: 0x7ff8151b0000,Image Size: 0x217000"
"3:12:22,5552525","median_filter.exe","22448","RegOpenKey","HKLM\System\CurrentContro
Access: Read"
"3:12:22,5552748","median_filter.exe","22448","RegOpenKey","HKLM\System\CurrentContro
Access: Read"
"3:12:22,5552958","median_filter.exe","22448","RegQueryValue","HKLM\System\CurrentCon
REG_SZ,Length: 10,Data: 1251"
"3:12:22,5553155","median_filter.exe","22448","RegQueryValue","HKLM\System\CurrentCon
REG_SZ,Length: 8,Data: 866"
"3:12:22,5553286","median_filter.exe","22448","RegCloseKey","HKLM\System\CurrentContro
```

"3:12:22,5564031","median_filter.exe","22448","CreateFile","C:\Users\kseni\lab2_OS_wi
Access: Execute/Traverse,Synchronize"
"3:12:22,5567324","median_filter.exe","22448","Load Image","C:\Windows\System32\kerne
Base: 0x7ff8146b0000,Image Size: 0xc4000"
"3:12:22,5570771","median_filter.exe","22448","Load Image","C:\Windows\System32\Kerne
Base: 0x7ff812940000,Image Size: 0x3b7000"
"3:12:22,5594092","median_filter.exe","22448","Load Image","C:\Windows\System32\msvcr
Base: 0x7ff8149e0000,Image Size: 0xa7000"
"3:12:22,5595299","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 19996"
"3:12:47,2253625","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 20312"
"3:12:47,2253925","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 9128"
"3:12:47,2254221","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 8096"
"3:12:47,2254497","median_filter.exe","22448","Thread Create","","SUCCESS","Thread
ID: 19576"
"3:12:52,5606885","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 19996,User Time: 0.0000000,Kernel Time: 0.0000000"
"3:13:17,2285648","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 9128,User Time: 0.0000000,Kernel Time: 0.0000000"
"3:13:17,2286066","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 8096,User Time: 0.0000000,Kernel Time: 0.0000000"
"3:13:17,2292343","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 19576,User Time: 0.0000000,Kernel Time: 0.0000000"
"3:13:17,2293547","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 20312,User Time: 0.0000000,Kernel Time: 0.0000000"
"3:13:17,2353137","median_filter.exe","22448","Thread Exit","","SUCCESS","Thread
ID: 10252,User Time: 0.0000000,Kernel Time: 0.0156250"
"3:13:17,2358070","median_filter.exe","22448","Process Exit","","SUCCESS","Exit
Status: 0,User Time: 0.0000000 seconds,Kernel Time: 0.0312500 seconds"
"3:13:17,2360930","median_filter.exe","22448","CloseFile","C:\Users\kseni\lab2_OS_wi

3 Лабораторная работа.

"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"23:43:40,6503020","parent.exe","20288","Process Start","","SUCCESS","Parent
PID: 18420,Command line: ""C:\Users\kseni\lab30SWaL\lab30S\build\bin\parent.exe"""
"23:43:40,6503115","parent.exe","20288","Thread Create","","SUCCESS","Thread
ID: 20272"
"23:43:40,6563945","parent.exe","20288","Load Image","C:\Users\kseni\lab30SWaL\lab30S
Base: 0x7ff60a250000,Image Size: 0xd8f000"
"23:43:40,6564545","parent.exe","20288","Load Image","C:\Windows\System32\ntdll.dll",
Base: 0x7ffbdcceb0000,Image Size: 0x217000"
"23:43:40,6574310","parent.exe","20288","CreateFile","C:\Users\kseni\lab30SWaL\lab30S
Access: Execute/Traverse,Synchronize"
"23:43:40,6575446","parent.exe","20288","Load Image","C:\Windows\System32\kernel32.dl

Base: 0x7ffbdbaf0000, Image Size: 0xc4000"
"23:43:40,6578340", "parent.exe", "20288", "Load Image", "C:\Windows\System32\KernelBase.dll"
Base: 0x7ffbda680000, Image Size: 0x3b7000"
"23:43:40,6643651", "parent.exe", "20288", "Load Image", "C:\Windows\System32\msvcrt.dll"
Base: 0x7ffbdbc20000, Image Size: 0xa7000"
"23:43:40,6644809", "parent.exe", "20288", "Thread Create", "", "SUCCESS", "Thread ID: 19752"
"23:43:40,6696331", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6697922", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6699217", "parent.exe", "20288", "Load Image", "C:\Windows\System32\sechost.dll"
Base: 0x7ffbdba40000, Image Size: 0xa8000"
"23:43:40,6700569", "parent.exe", "20288", "Load Image", "C:\Windows\System32\bcrypt.dll"
Base: 0x7ffbdabb0000, Image Size: 0x28000"
"23:43:40,6701619", "parent.exe", "20288", "Thread Create", "", "SUCCESS", "Thread ID: 20352"
"23:43:40,6707927", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize"
"23:43:40,6734533", "parent.exe", "20288", "Process Create", "C:\Users\kseni\lab30SWaL\lab304, Command line: child1.exe parent_to_child1 child1_to_child2"
"23:43:40,6793554", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6794965", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Generic Read/Execute"
"23:43:40,6824945", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6828197", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6831317", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize"
"23:43:40,6901308", "parent.exe", "20288", "Process Create", "C:\Users\kseni\lab30SWaL\lab3040, Command line: child2.exe child1_to_child2 child2_to_parent"
"23:43:40,6960682", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Generic Read"
"23:43:40,6962319", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Read Attributes"
"23:43:40,6963647", "parent.exe", "20288", "CreateFile", "C:\Users\kseni\lab30SWaL\lab30S Access: Generic Read/Execute"
"23:44:10,6672035", "parent.exe", "20288", "Thread Exit", "", "SUCCESS", "Thread ID: 20352, User Time: 0.0000000, Kernel Time: 0.0000000"
"23:44:10,6672537", "parent.exe", "20288", "Thread Exit", "", "SUCCESS", "Thread ID: 19752, User Time: 0.0000000, Kernel Time: 0.0000000"
"23:44:24,5527866", "parent.exe", "20288", "Thread Exit", "", "SUCCESS", "Thread ID: 20272, User Time: 0.0000000, Kernel Time: 0.0000000"
"23:44:24,5532847", "parent.exe", "20288", "Process Exit", "", "SUCCESS", "Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0000000 seconds"
"23:44:24,5535345", "parent.exe", "20288", "CloseFile", "C:\Users\kseni\lab30SWaL\lab30S

4 Лабораторная работа. Программа 1.

```
"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"17:09:14,7530688","Program1.exe","20912","Process Start","","SUCCESS","Parent
PID: 21036,Command line: ""C:\Users\kseni\lab4_OS\build\Program1.exe"""
"17:09:14,7530801","Program1.exe","20912","Thread Create","","SUCCESS","Thread
ID: 1684"
"17:09:14,7563884","Program1.exe","20912","Load Image","C:\Users\kseni\lab4_OS\build\
Base: 0x7ff60d9a0000,Image Size: 0xe77000"
"17:09:14,7564439","Program1.exe","20912","Load Image","C:\Windows\System32\ntdll.dll
Base: 0x7ffcfcf190000,Image Size: 0x217000"
"17:09:14,7575445","Program1.exe","20912","CreateFile","C:\Users\kseni\lab4_OS\build\
Access: Execute/Traverse,Synchronize"
"17:09:14,7576813","Program1.exe","20912","Load Image","C:\Windows\System32\kernel32.
Base: 0x7fffcfe350000,Image Size: 0xc4000"
"17:09:14,7578457","Program1.exe","20912","Load Image","C:\Windows\System32\KernelBas
Base: 0x7ffcf790000,Image Size: 0x3b7000"
"17:09:14,7606672","Program1.exe","20912","Load Image","C:\Windows\System32\msvcrt.dl
Base: 0x7fffcfe150000,Image Size: 0xa7000"
"17:09:14,7607882","Program1.exe","20912","Thread Create","","SUCCESS","Thread
ID: 16056"
"17:09:14,7610630","Program1.exe","20912","Thread Create","","SUCCESS","Thread
ID: 3904"
"17:09:14,7611324","Program1.exe","20912","CreateFile","C:\Users\kseni\lab4_OS\build\
Access: Read Attributes"
"17:09:14,7612845","Program1.exe","20912","CreateFile","C:\Users\kseni\lab4_OS\build\
Access: Read Data/List Directory,Execute/Traverse,Synchronize"
"17:09:14,7615829","Program1.exe","20912","Load Image","C:\Users\kseni\lab4_OS\build\
Base: 0x7ffcebd80000,Image Size: 0xc8000"
"17:09:34,8704094","Program1.exe","20912","Thread Exit","","SUCCESS","Thread
ID: 3904,User Time: 0.0000000,Kernel Time: 0.0000000"
"17:09:34,8704341","Program1.exe","20912","Thread Exit","","SUCCESS","Thread
ID: 16056,User Time: 0.0000000,Kernel Time: 0.0000000"
"17:09:34,8705034","Program1.exe","20912","Thread Exit","","SUCCESS","Thread
ID: 1684,User Time: 0.0000000,Kernel Time: 0.0000000"
"17:09:34,8707727","Program1.exe","20912","Process Exit","","SUCCESS","Exit
Status: 0,User Time: 0.0000000 seconds,Kernel Time: 0.0000000 seconds"
"17:09:34,8709014","Program1.exe","20912","CloseFile","C:\Users\kseni\lab4_OS\build",
```

4 Лабораторная работа. Программа 2.

```
"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"17:11:00,9458735","Program2.exe","8972","Process Start","","SUCCESS","Parent
PID: 21036,Command line: ""C:\Users\kseni\lab4_OS\build\Program2.exe"""
"17:11:00,9458927","Program2.exe","8972","Thread Create","","SUCCESS","Thread
ID: 340"
"17:11:00,9486890","Program2.exe","8972","Load Image","C:\Users\kseni\lab4_OS\build\P
```

Base: 0x7ff74f4c0000, Image Size: 0xe77000"
"17:11:00,9487563", "Program2.exe", "8972", "Load Image", "C:\Windows\System32\ntdll.dll"
Base: 0x7ffc90000, Image Size: 0x217000"
"17:11:00,9498644", "Program2.exe", "8972", "Load Image", "C:\Windows\System32\kernel32.dll"
Base: 0x7ffcf350000, Image Size: 0xc4000"
"17:11:00,9500466", "Program2.exe", "8972", "Load Image", "C:\Windows\System32\KernelBase.dll"
Base: 0x7ffcf790000, Image Size: 0x3b7000"
"17:11:00,9520963", "Program2.exe", "8972", "Load Image", "C:\Windows\System32\msvcrt.dll"
Base: 0x7ffcf150000, Image Size: 0xa7000"
"17:11:00,9522227", "Program2.exe", "8972", "Thread Create", "", "SUCCESS", "Thread ID: 10696"
"17:11:00,9532480", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Attributes"
"17:11:00,9532787", "Program2.exe", "8972", "QueryBasicInformationFile", "C:\Users\kseni\lab4_OS\1",
08.12.2025 16:09:58, LastWriteTime: 08.12.2025 17:02:52"
"17:11:00,9533083", "Program2.exe", "8972", "CloseFile", "C:\Users\kseni\lab4_OS\build\1",
"17:11:00,9534164", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Data/List Directory, Execute/Traverse"
"17:11:00,9534632", "Program2.exe", "8972", "CreateFileMapping", "C:\Users\kseni\lab4_OS\1",
LOCKED WITH ONLY READERS", "PageProtection: PAGE_EXECUTE_READ|PAGE_NOCACHE"
"17:11:00,9535635", "Program2.exe", "8972", "CreateFileMapping", "C:\Users\kseni\lab4_OS\1",
SyncTypeOther"
"17:11:00,9537398", "Program2.exe", "8972", "Load Image", "C:\Users\kseni\lab4_OS\build\1",
Base: 0x7ffca2580000, Image Size: 0xc8000"
"17:11:00,9538258", "Program2.exe", "8972", "CloseFile", "C:\Users\kseni\lab4_OS\build\1",
"17:11:06,3636601", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Attributes"
"17:11:06,3636927", "Program2.exe", "8972", "QueryBasicInformationFile", "C:\Users\kseni\lab4_OS\1",
08.12.2025 16:09:58, LastWriteTime: 08.12.2025 17:02:52"
"17:11:06,3637054", "Program2.exe", "8972", "CloseFile", "C:\Users\kseni\lab4_OS\build\1",
"17:11:06,3637774", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Data/List Directory, Execute/Traverse"
"17:11:06,3638156", "Program2.exe", "8972", "CreateFileMapping", "C:\Users\kseni\lab4_OS\1",
LOCKED WITH ONLY READERS", "PageProtection: PAGE_EXECUTE_READ|PAGE_NOCACHE"
"17:11:06,3638855", "Program2.exe", "8972", "CreateFileMapping", "C:\Users\kseni\lab4_OS\1",
SyncTypeOther"
"17:11:06,3641161", "Program2.exe", "8972", "Load Image", "C:\Users\kseni\lab4_OS\build\1",
Base: 0x7ffca2580000, Image Size: 0xc8000"
"17:11:06,3642129", "Program2.exe", "8972", "CloseFile", "C:\Users\kseni\lab4_OS\build\1",
"17:11:10,2538977", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Attributes"
"17:11:10,2539282", "Program2.exe", "8972", "QueryBasicInformationFile", "C:\Users\kseni\lab4_OS\1",
08.12.2025 16:09:58, LastWriteTime: 08.12.2025 17:02:52"
"17:11:10,2539411", "Program2.exe", "8972", "CloseFile", "C:\Users\kseni\lab4_OS\build\1",
"17:11:10,2540129", "Program2.exe", "8972", "CreateFile", "C:\Users\kseni\lab4_OS\build\1",
Access: Read Data/List Directory, Execute/Traverse"
"17:11:10,2540502", "Program2.exe", "8972", "CreateFileMapping", "C:\Users\kseni\lab4_OS\1",
LOCKED WITH ONLY READERS", "PageProtection: PAGE_EXECUTE_READ|PAGE_NOCACHE"

"17:11:10,2541108","Program2.exe","8972","CreateFileMapping","C:\Users\kseni\lab4_OS\SyncTypeOther"
"17:11:10,2542536","Program2.exe","8972","Load Image","C:\Users\kseni\lab4_OS\build\1
Base: 0x7ffca2580000, Image Size: 0xc8000"
"17:11:10,2544272","Program2.exe","8972","CloseFile","C:\Users\kseni\lab4_OS\build\li
"17:11:24,0989416","Program2.exe","8972","Thread Exit","","SUCCESS","Thread
ID: 10696"
"17:11:24,0989960","Program2.exe","8972","Thread Exit","","SUCCESS","Thread
ID: 340"
"17:11:24,0992375","Program2.exe","8972","Process Exit","","SUCCESS","Exit
Status: 0"