**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**Факультет прикладной математики – процессов управления**

**отчет**

**по лабораторной работе**

**по дисциплине «Системное программирование в Linux»**

**на тему «Разработка системного инструмента для аудита системы»**

|  |  |  |
| --- | --- | --- |
| Студент гр. 22.Б15 |  | Агишев А.Б. |
| Преподаватель |  | Киямов Ж.У. |

**Санкт-Петербург**

**2023 г.**

**Содержание**

[1. Цель работы 2](#_Toc154235591)

[2. Задача 2](#_Toc154235592)

[3. Теоретическая часть 2](#_Toc154235593)

[4. Алгоритм метода 3](#_Toc154235594)

[5. Описание программы 4](#_Toc154235595)

[6. Рекомендации пользователю 4](#_Toc154235596)

[7. Рекомендации программисту 4](#_Toc154235597)

[8. Контрольный пример 5](#_Toc154235598)

[9. Заключение 6](#_Toc154235599)

[10. Литература 6](#_Toc154235600)

# **Цель работы**

Разработать системный инструмент, который будет использоваться для аудита и мониторинга системы Linux.

# **Задача**

1. Определить список системных вызовов.
2. Написать программу для аудита и мониторинга.
3. Проверить работоспособность программмы

# **Теоретическая часть**

Аудит и мониторинг системы Linux представляют собой процессы наблюдения и анализа активности в операционной системе Linux с целью обеспечения безопасности, целостности данных и эффективности работы системы.

*Аудит*:

Определение событий: Наблюдение за различными событиями в системе, такими как системные вызовы, файловые операции, аутентификация и другие действия пользователей.

Запись событий: Фиксирование информации о событиях в аудиторских журналах для последующего анализа.

Анализ событий: Анализ журналов аудита для выявления потенциальных угроз безопасности и отслеживания активности пользователей.

*Мониторинг*:

Слежение за ресурсами: Отслеживание использования системных ресурсов, таких как ЦП, память, сеть и диски, для обеспечения эффективности и предотвращения проблем.

Анализ производительности: Оценка производительности системы, выявление узких мест и оптимизация работы приложений.

Выявление нештатных ситуаций: Мониторинг для обнаружения отклонений от нормального функционирования, таких как сбои в работе приложений или аномальное использование ресурсов.

# **Алгоритм метода**

Программа состоит из следующих частей:

1. Получение PID процесса.

# **Описание программы**

Описание функций программы *«chess.cpp»* представлено в таблице 5.1.

*Таблица 5.1. Описание функций программы «chess.cpp»*

|  |  |  |
| --- | --- | --- |
| Входные данные | Имя | Описание |
| Доска | show\_board | Показ доски |
| Доска | rotate\_board | Поворот доски |
| Координаты | on\_the\_border | Проверка что фигура не выходит за пределы доски |
| Доска, координаты | make\_moves | Создание движений для фигур |
| Доска, игрок | is\_check | Проверка шаха |
| Доска | is\_checkmate | Проверка мата |
| Доска, количество движений, параметры | generate\_moves | Генерация доски |
| Доска, координаты | calculate\_score | Вычисление количества очков |
| Доска, количество ходов, ходы | find\_best\_moves\_recursive | Рекурсивный поиск лучших ходов |
| - | main | Запуск |

# **Рекомендации пользователю**

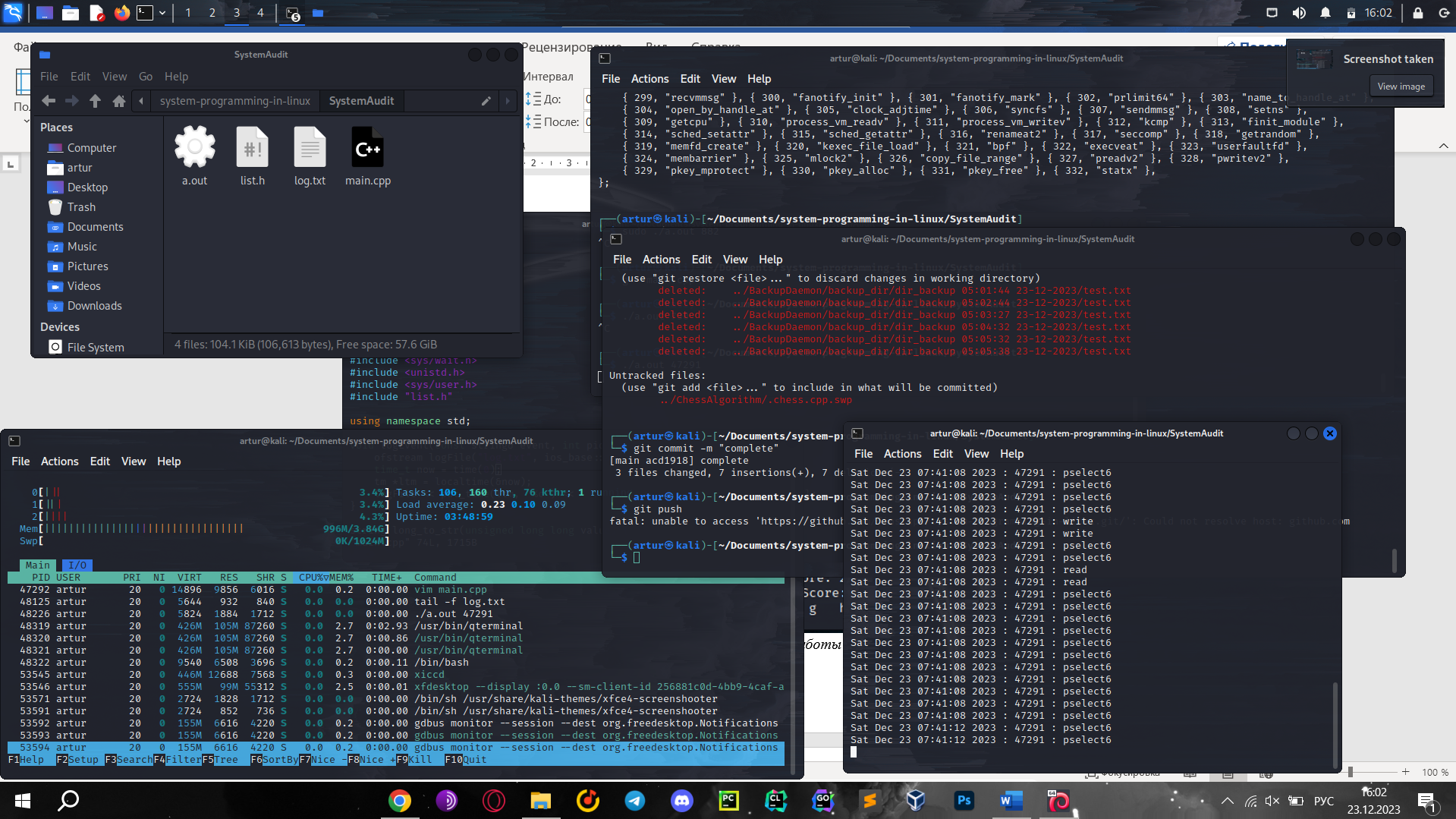
Скомпилируйте программу и введите PID процесса.

# **Рекомендации программисту**

Для запуска программы необходим C++ 20. Запускать только на Linux.

Библиотеки: string, fstream, iostream, ctime, vector, iomanip, sys/ptrace, sys/types, sys/wait, unistd, sys/user

# **Контрольный пример**



*Рисунок 8.1 Пример работы программы.*

# **Заключение**

В результате выполнения работы был разработан системный инструмент для аудита и мониторинга системы Linux. Этот инструмент включает в себя определение списка системных вызовов, написание программы для аудита и мониторинга, а также проверку её работоспособности.

# **Литература**

1. <https://github.com/finstape/system-programming-in-linux>