**Санкт-Петербургский государственный УНИВЕРСИТЕТ**

**Факультет прикладной математики и процессов управления**

**отчет**

**по лабораторной работе №3**

**по дисциплине «Программирование в Линукс»**

**на тему «Создание аудита системных событий»**

|  |  |  |
| --- | --- | --- |
| Студент гр. 22Б15 |  | Суворов Н.В. |
| Преподаватель |  | Киямов Ж.У. |

**Санкт-Петербург**

**2023 г.**

**Оглавление**

[1. Цель 3](#_Toc152350215)

[2. Задача 3](#_Toc152350216)

[3. Теория 3](#_Toc152350217)

[5. Рекомендации программиста 3](#_Toc152350218)

[6. Рекомендации пользователя 4](#_Toc152350219)

[7. Пример 4](#_Toc152350220)

[8. Вывод 5](#_Toc152350221)

[9. Литература 5](#_Toc152350222)

# Цель

Создать программу аудита системных событий.

# Задача

1. Написать код программы на c++
2. Добавит возможность логирования.

# Теория

Аудит в Linux - это процесс мониторинга и контроля за событиями и действиями, происходящими в операционной системе. Он направлен на обеспечение безопасности, выявление уязвимостей и анализ событий в системе с целью обеспечения соответствия политике безопасности и выявления возможных аномалий или несанкционированных действий.

Программы аудита в Linux позволяют анализировать журналы событий, регистрировать и анализировать различные виды активности, такие как доступ к файлам, запуск программ, изменения конфигураций и другие действия, чтобы обеспечить более высокий уровень безопасности и интегритета системы.

1. **Входные данные и решение**

GitHub https://github.com/AlexShinalov/Linux/tree/main/course%202/Audit

*Таблица 4.1 Функции*

|  |  |
| --- | --- |
| Название | Назначение |
| current\_time | Сохраняет локальное время |
| write\_system | Записывает файл |
| write\_command | Записывает команды |
| main | Основной код |

# Рекомендации программиста

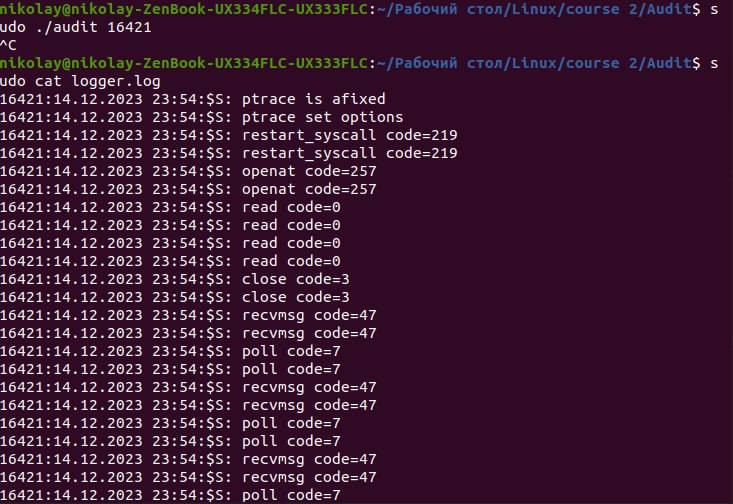
Для запуска программы необходима версия g++ не ниже 5.1. Также желательно иметь права суперпользователя в системе и иметь представления о базовых командах в linux.

# Рекомендации пользователя

Следуйте инструкциям на GitHub для корректной установки программы.

# Пример

После запуска программы мы получаем сведенья о процессе 16241 (chrome). Вся информация на период прослушивания сохранилась в файл logs.log



*Рисунок 7.1*

# Вывод

В результате выполнения работы была разработана программа-аудит для мониторинга системных событий в Linux. Также были получены все необходимые сведения о разработке подобных программ.

# Литература

<https://habr.com/ru/companies/selectel/articles/267833/>

<https://xakep.ru/2021/09/16/linux-audit/>