АНОТАЦІЯ

Кваліфікаційна робота включає пояснювальну записку (58 с., 25 рис., 4 додатки).

Об’єктом розробки є процес збору інформації про системні виклики для операційної системи Linux.

Предметом розробки є драйвер для системи Linux, який встановлює користувацькі обробники системних викликів, які в режимі реального часу збирають і записують інформацію, а саме шлях до виконуваного файлу процесу і шлях до файлу, з яким виконується дія в системному виклику

Розроблений драйвер надає:

* + можливість встановлення користувацького обробника на певні системні виклики в залежності від встановленого рівня;
  + можливість змінити визначений рівень, тобто зміни групи системних викликів які відслідковуються;
  + можливість заборони запуску певного процесу за шляхом до виконуючого файлу;
  + передбачена можливість зупинки і поновлення запису зібраної інформації в журнал ядра.

В процесі розробки була використана мова програмування C, без жодної сторонньої бібліотеки

В ході виконання дипломного проєкту:

* + проведений аналіз існуючих рішень;
  + розроблено драйвер;
  + розроблено інтерфейс для програмістів, для взаємодії з драйвером.

Використання цього драйвера, допоможе відслідковувати роботу системних викликів, переглядати зібрану інформацію, а також блокувати запуск певних процесів.

Ключові слова: ДРАЙВЕР LINUX, C, СИСТЕМНІ ВИКЛИКИ, КОРИСТУВАЦЬКИЙ ОБРОБНИК СИСТЕМНИХ ВИКЛИКІВ, ПРОЦЕСИ, ЛОГУВАННЯ.

ABSTRACT

The qualification work includes an explanatory note (58 p., 25 figures, 4 appendices).

The object of development is the process of collecting information about system calls for the Linux operating system.

The subject of the development is a driver for the Linux system that installs custom system call handlers that collect and record information in real time, namely the path to the executable file of the process and the path to the file with which the action in the system call is performed

The developed driver provides:

• the ability to install a custom handler for certain system calls depending on the set level;

• the ability to change the specified level, that is, changes in the group of system calls that are monitored;

• the possibility of prohibiting the launch of a certain process based on the path to the executable file;

• the possibility of stopping and resuming the recording of collected information in the kernel log is provided.

The C programming language was used in the development process, without any third-party libraries

During the implementation of the diploma project:

• an analysis of existing solutions was carried out;

• a driver was developed;

• developed an interface for the interaction of programmers with the driver.

Using this driver will help monitor the operation of system calls, view the collected information, and also block the launch of certain processes.

Keywords: LINUX DRIVER, C, SYSTEM CALLS, USER SYSTEM CALL HANDLER, PROCESSES, LOGGING.