# Лабораторная работа № 2 – Реализация моделей безопасности в ОС Windows

## Цель работы

Исследование принципов разработки моделей безопасности, функционирующих на уровне ядра ОС Windows.

## Формулировка задания

Разработать драйвер-фильтр для ОС Windows 7/8/8.1/10, позволяющий ограничить права доступа процессов к объектам файловой системы. Разграничение должно осуществляться по правилам Дискреционной модели доступа/Ролевой модели доступа (в зависимости от варианта).

В ходе выполнения лабораторной работы необходимо выполнить следующие действия:

1. Исследовать методы разработки драйверов для ОС Windows, изучить типы драйверов файловой системы, выбрать подходящий тип драйвера.
2. Подготовить среду разработки, которая включает в себя Visual Studio, Window Driver Kit (WDK), Software Development Kit (SDK).
3. Подготовить целевую ОС, на которой будет работать разработанный драйвер, для возможности установки неподписанных драйверов.
4. Изучить существующие проекты драйверов. Выбрать наиболее подходящий для поставленной задачи и скомпилировать его.
5. Разработать простейшую программу, позволяющую читать и записывать в текстовый файл данные. Название файла и данные для записи подаются в качестве аргументов командной строки.
6. Доработать выбранный драйвер до возможности блокировки запросов от процессов к файлам в определенной директории. Доступ процесса к файлу должен определяться моделью контроля доступа и правами,

указанными в отдельном текстовом файле (конфигурационный файл). В качестве процесса выступает разработанная в п.5 программа.

## Список источников


1. https://learn.microsoft.com/ru-ru/windows-hardware/drivers/download-the-wdk
2. https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/
3. https://github.com/microsoft/Windows-driver-samples
4. https://www.howtogeek.com/167723/how-to-disable-driver-signature-verification-on-64-bit-windows-8.1-so-that-you-can-install-unsigned-drivers/