

С.А. Захаров

В последнее время наметилась тенденция обновления парка вычислительных машин в школах и университетах республики. Новые поставки техники включают компьютеры нового поколения, которые позволяют устанавливать операционную систему Windows 95 или Windows 98. В связи с большим количеством работающих на рабочей станции пользователей возникает проблема защиты важных файлов системы от удаления или модификации их пользователями или другими программами, что может привести к неправильной работе операционной системы, и даже к ее выходу из рабочего состояния. Так же остро стоит проблема защиты файлов пользователей от их удаления или изменения без ведома их владельца. Задачей данного проекта была разработка и отладка программного средства выполняющего защиту файлов и каталогов, и настройку системы. Программа защиты реализована в виде vxd-драйвера, позволяющего использовать системные вызовы самого низкого уровня. Это гарантирует программе высокую защиту, программа не видна ни в одном из списков процессов, так как и не является процессом, отсюда следует, что ее невозможно выгрузить из памяти различными программами, которые могут редактировать списки запущенных процессов. Интерфейс управления настроек драйвера исполнен в виде Delphi-проекта, он интуитивно прост и понятен для пользователя и взаимодействует с драйвером, используя зашифрованные вызовы, что бы исключить возможность проследить их и воспроизвести из других программ.

Загрузка программы происходит на ранней стадии загрузки операционной системы что делает невозможным ее снятия при старте, так как еще не загрузился GUI интерфейс.

В программе реализована функция динамической загрузки и выгрузки виртуального драйвера, что обеспечивает изменение параметров программы без перезагрузки компьютера.

Вся критически важная информация о программе хранится не в конфигурационных файлах, а в различных разделах реестра.

Данный проект был протестирован, а затем внедрен и успешно используется на рабочих станциях в Гомельском государственном областном лицее.