БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

ИИТ БГУИР

Программное обеспечение информационных технологий.

Дисциплина: «Сетевые технологии и администрирование операционных систем»

Отчет

По лабораторной работе №6

«Hooks»

Выполнил студент группы 681072: Иванов К.Е.

Проверил преподаватель: Калитеня И.Л.

Минск 2019

**Задание:** Разработать программу, которая запускает приложение, переданное программе на вход. После запуска приложения должна выполняться журнализация всех обращений приложения к реестру и файловой системе. Для этого в запущенное приложение должна подгружаться DLL-библиотека, перехватывающая функции работы с файловой системой (NtXxxx). Перехват обращений к реестру можно осуществить любым известным способом.

**Код приложения:**

#include <vcl.h>

#pragma hdrstop

#include "Unit1.h"

#include "Registry.hpp"

//---------------------------------------------------------------------------

#pragma package(smart\_init)

#pragma resource "\*.dfm"

TForm1 \*Form1;

//---------------------------------------------------------------------------

\_\_fastcall TForm1::TForm1(TComponent\* Owner)

: TForm(Owner)

{

}

//---------------------------------------------------------------------------

void \_\_fastcall TForm1::btn2Click(TObject \*Sender)

{

if (this->edt1->Text.Length()) {

TRegistry \*reg=new TRegistry(); //Создали обьект reg класса TRegistry

reg->RootKey=HKEY\_CURRENT\_USER; //Для начала необходимо указать раздел, с которым мы будем работать (список всех разделов был приведен выше).

//В нашем случае это будет HKEY\_CURRENT\_USER, который стоит по умолчанию

//Теперь нам нужно указать ключ реестра, в который будет происходить запись.

reg->OpenKey("\NitanTest",true); //Мы создали ключ, если же такой ключ уже существовал, то он был бы открыт для записи

reg->WriteString("MyName",this->edt1->Text); //Теперь мы записали параметр MyName и задали ему значение Nitan

reg->CloseKey(); //Закрываем ключ

delete reg; //Освобождаем память

//Можно открыть реестр и полюбоваться на проделанную работу.

this->mmo1->Lines->Clear();

this->mmo1->Lines->Add("WriteRegistry");

this->mmo1->SelectAll();

this->mmo1->CopyToClipboard();

}

}

//---------------------------------------------------------------------------

void \_\_fastcall TForm1::btn1Click(TObject \*Sender)

{

TRegistry \*reg=new TRegistry(); //Создали обьект reg класса TRegistry

reg->RootKey=HKEY\_CURRENT\_USER; //Как и при записи указываем раздел с которым будем работать

reg->OpenKeyReadOnly("NitanTest"); //Теперь открываем ключ для чтения (можно было бы и использовать OpenKey(), но эта функция позволяет только читать параметры )

this->edt2->Text = reg->ReadString("MyName"); //Заносим значение, указан при этом нужный нам параметр

//Любуемся правильным результатом

reg->CloseKey(); //Закрываем ключ

delete reg; //Освобождаем память

this->mmo1->Lines->Clear();

this->mmo1->Lines->Add("ReadRegistry");

this->mmo1->SelectAll();

this->mmo1->CopyToClipboard();

}

//---------------------------------------------------------------------------