Министерство образование Российской Федерации

Пензенский государственный университет

Кафедра «Вычислительная техника»

**ОТЧЕТ**

по лабораторной работе № 5

по курсу «Защита информации в сети Internet»

«Атрибуты безопасности в ОС Windows»

Выполнили студенты группы 18ВВ1:

Гаевский И.

Воеков И.

Немцев А.

Приняли:  
к.т.н., доцент Дубравин А.В.

к.т.н., доцент Карамышева Н.С.

Пенза 2020

### Цель работы

### Изучить методы работы с атрибутами безопасности в ОС Windows.

### Лабораторное задание

Разработать программу, выполняющую создание файла с атрибутами безопасности для группы пользователей «Администраторы» и правами на изменение и запись, а для группы пользователей «Все» следует запретить чтение и исполнение.

**Листинг**

#include <Windows.h>

#include <AccCtrl.h>

#include <Aclapi.h>

#include <conio.h>

#include <stdio.h>

int main()

{

// Объявляем структуру EXPLICIT\_ACCESS для двух групп

EXPLICIT\_ACCESS ea[2];

// Предварительно обнуляем

ZeroMemory(&ea, 2 \* sizeof(EXPLICIT\_ACCESS));

// Получение идентификатора группы Everyone

SID\_IDENTIFIER\_AUTHORITY SIDAuthWorld = SECURITY\_WORLD\_SID\_AUTHORITY;

PSID pEveryoneSID = NULL;

if (!AllocateAndInitializeSid(

&SIDAuthWorld,

1,

SECURITY\_WORLD\_RID,

0, 0, 0, 0, 0, 0, 0,

&pEveryoneSID)) {

printf("AllocateAndInitializeSid Error");

}

// Заполнение структуры EXPLICIT\_ACCESS для группы Everyone

ea[0].grfAccessPermissions = GENERIC\_READ | GENERIC\_EXECUTE; // Права на чтение и исполнение

ea[0].grfAccessMode = DENY\_ACCESS; // Запретить

ea[0].grfInheritance = NO\_INHERITANCE;

ea[0].Trustee.TrusteeForm = TRUSTEE\_IS\_SID;

ea[0].Trustee.TrusteeType = TRUSTEE\_IS\_WELL\_KNOWN\_GROUP; // Для группы

ea[0].Trustee.ptstrName = (LPWSTR)pEveryoneSID;

//получение идентификатора группы Администраторы

SID\_IDENTIFIER\_AUTHORITY SIDAuthAdmin = SECURITY\_NT\_AUTHORITY;

PSID pAdminSID = NULL;

if (!AllocateAndInitializeSid(&SIDAuthAdmin, 2,

SECURITY\_BUILTIN\_DOMAIN\_RID,

DOMAIN\_ALIAS\_RID\_ADMINS,

0, 0, 0, 0, 0, 0,

&pAdminSID)){

printf("AllocateAndInitializeSid Error %u\n", GetLastError());

return FALSE;

}

// Заполнение структуры EXPLICIT\_ACCESS для группы Администраторы

ea[1].grfAccessPermissions = GENERIC\_WRITE; // Права на запись

ea[1].grfAccessMode = SET\_ACCESS; // Разрешить

ea[1].grfInheritance = NO\_INHERITANCE;

ea[1].Trustee.TrusteeForm = TRUSTEE\_IS\_SID;

ea[1].Trustee.TrusteeType = TRUSTEE\_IS\_WELL\_KNOWN\_GROUP; // Для группы

ea[1].Trustee.ptstrName = (LPWSTR)pAdminSID;

// Генерируется новый список ACL

PACL pACL = NULL;

DWORD dwRes = SetEntriesInAcl(2, ea, NULL, &pACL);

if (dwRes != ERROR\_SUCCESS) {

FreeSid(pEveryoneSID);

FreeSid(pAdminSID);

printf("SetEntriesInAcl Error");

}

// Выделяем память под дескриптор безопасности

PSECURITY\_DESCRIPTOR pSD = (PSECURITY\_DESCRIPTOR)LocalAlloc(LPTR, SECURITY\_DESCRIPTOR\_MIN\_LENGTH);

if (pSD == NULL) {

FreeSid(pEveryoneSID);

FreeSid(pAdminSID);

LocalFree(pACL);

printf("LocalAlloc Error");

}

// Инициализируем дескриптор безопасности

if (!InitializeSecurityDescriptor(pSD, SECURITY\_DESCRIPTOR\_REVISION)) {

FreeSid(pEveryoneSID);

FreeSid(pAdminSID);

if(pACL)LocalFree(pACL);

LocalFree(pSD);

printf("InitializeSecurityDescriptor Error");

}

if (!SetSecurityDescriptorDacl(pSD, TRUE, pACL, FALSE)) {

FreeSid(pEveryoneSID);

FreeSid(pAdminSID);

LocalFree(pACL);

LocalFree(pSD);

printf("SetSecurityDescriptorDacl Error");

}

// Теперь, когда дескриптор безопасности создан,

// его можно использовать при создание файла, заполнив структуру SECURITY\_ATTRIBUTES

SECURITY\_ATTRIBUTES sa;

sa.nLength = sizeof(SECURITY\_ATTRIBUTES);

sa.lpSecurityDescriptor = pSD;

sa.bInheritHandle = FALSE;

HANDLE hFile = CreateFile(L"test.txt", GENERIC\_ALL, NULL, &sa, CREATE\_NEW, FILE\_ATTRIBUTE\_NORMAL, NULL);

if (hFile){

printf("Done! Check test.txt! ");

}

else{

printf("Error! File not created!");

}

FreeSid(pEveryoneSID);

FreeSid(pAdminSID);

LocalFree(pACL);

LocalFree(pSD);

int gch = \_getch();

}

**Результат работы программы**

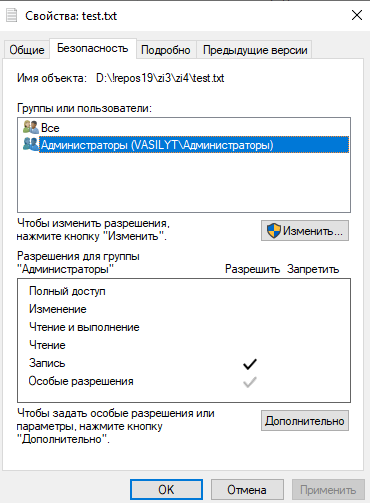
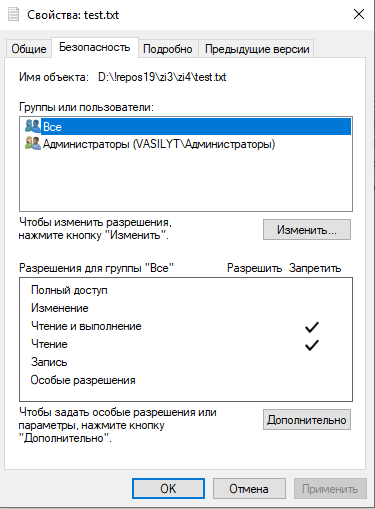
 

Рисунок 2 - Атрибуты безопасности файла

**Вывод**

Изучили методы работы с атрибутами безопасности в ОС Windows.