

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №4**

**з дисципліни «Безпека програм та даних»**

**на тему: «Списки контролю доступу Access-Contol List»**

Виконав: ???

Прийняв: ???

Дніпро, 2023

**Тема**: Списки контролю доступу Access-Contol List (ACL).

**Мета**: Ознайомитися із списками контролю доступу.

**Завдання**:

Написати програму відповідно до заданого варіанту. Встановити права доступу до наступних об’єктів:

|  |  |
| --- | --- |
| Варіант | Завдання |
| 11 | Заборонити читання файлу |

**Короткі теоретичні відомості**:

Security descriptor містить інформацію про власника об'єкту, а також може включати наступні списки контролю доступу Access-Contol List (ACL): ACL - асces control list - фундаментальна частина Windows NT .

ACL визначає, який у вас доступ на ті або інші ресурси .Складається з 2-х частин : 1.

1) DACL - визначає права доступу до ресурсів

2) SACL - контролює ці права.

Наступний код визначає, чи розповсюджується ACL на диск С

#include "stdafx.h"

#include "stdio.h"

#include <windows.h>

int main()

{ char \* vol = "з:\\";

DWORD f = 0 ;

if(GetVolumeInformation(vo1,NULL,0,NULL,NULL,&f,NULL,0))

{ printf ("%s support ACLs",vo1,(f & FS\_PERSISTENT\_ACLS)? "" : "NOT");

}

else { printf ("error");

}

return 0;

}

DACL складається з одного або декількох АСІ - асcess control entries .

АСІ складається з SID (Security ID) - і описи того, що може робити цей SID з ресурсом.SID представляє користувача, групу або комп'ютер. Наприклад, якщо аккаунт, який визначає ваші права на ресурс, є EveryOne (Deny Full Control), то SID = S-1-1-0 . Кожний дескриптор має свій опис, який можна знайти в sddl.h .

**Текст програми:**

#include <iostream>

#include <sys/types.h>

#include <sys/stat.h>

#include <io.h>

#include <stdio.h>

#include <stdlib.h>

#include <errno.h>

void set\_mode\_and\_report(const char\* filename, int mask)

{

// если не удается найти файл или неверный параметр доступа

if (\_chmod(filename, mask) == -1)

{

switch (errno)

{

case EINVAL:

fprintf(stderr, "Неверный параметр доступа.\n");

break;

case ENOENT:

fprintf(stderr, "Не удается найти файл.\n");

break;

default:

//никогда не будет достигнута

fprintf(stderr, "Непредвиденная ошибка.\n");

}

}

else

{

if (mask == \_S\_IREAD)

printf("Режим файла изменен: запрет на запись.\n");

else if (mask & \_S\_IWRITE)

printf("Режим файла изменен: чтение и запись.\n");

else if (mask == 0)

printf("Режим файла изменен: запрет на чтение и запись.\n");

}

fflush(stderr);

}

int main()

{

setlocale(LC\_ALL, "Rus");

// создаю файл и пробую его прочесть

if (system("echo /\* End of file \*/ >> crt\_chmod.c\_input") == 1)

{

printf("Не удалось создать и открыть файл.\n");

}

else printf("Файл успешно создан, открыт и изменен.\n");

// запрещаю чтение файла

set\_mode\_and\_report("crt\_chmod.c\_input ", 0);

//пробую прочесть файл

if (system("echo /\* End of file \*/ >> crt\_chmod.c\_input") == 1)

{

printf("Не удалось открыть файл.\n");

}

else printf("Файл успешно открыт и изменен.\n");

//разрешаю чтение файла

set\_mode\_and\_report("crt\_chmod.c\_input ", \_S\_IWRITE);

//пробую прочесть файл

if (system("echo /\* End of file \*/ >> crt\_chmod.c\_input") == 1)

{

printf("Не удалось открыть файл.\n");

}

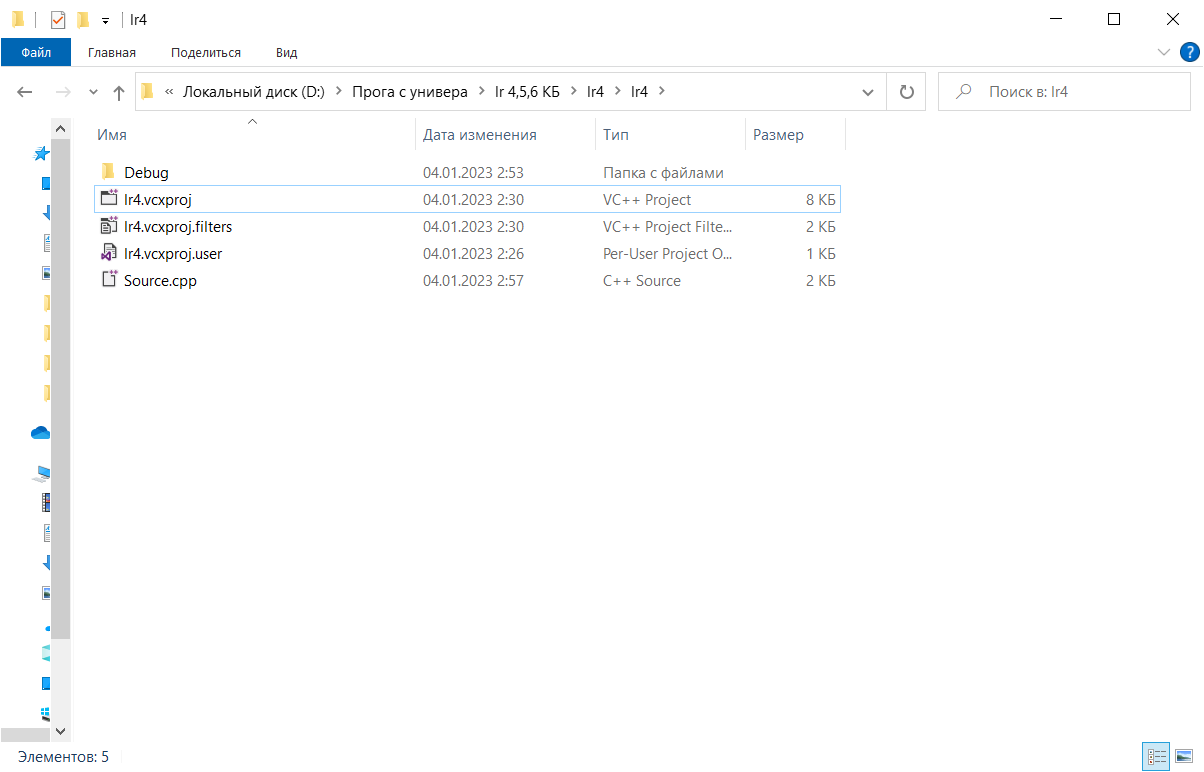
else printf("Файл успешно открыт и изменен.\n");

return 0;

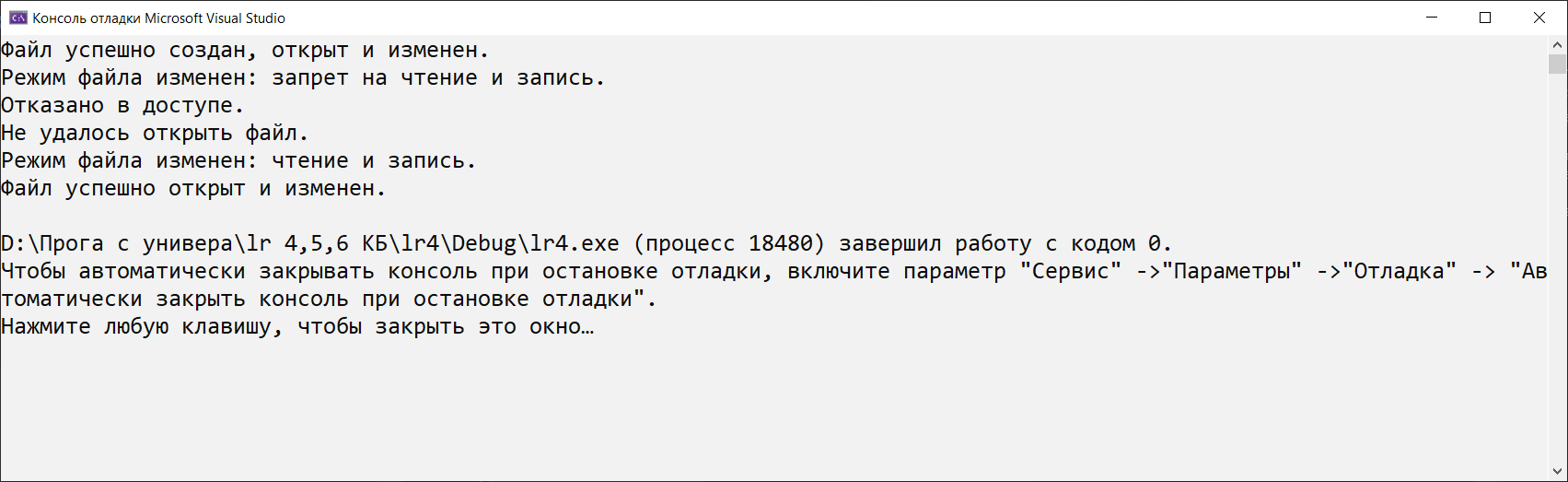
}

**Результати виконання програми:**

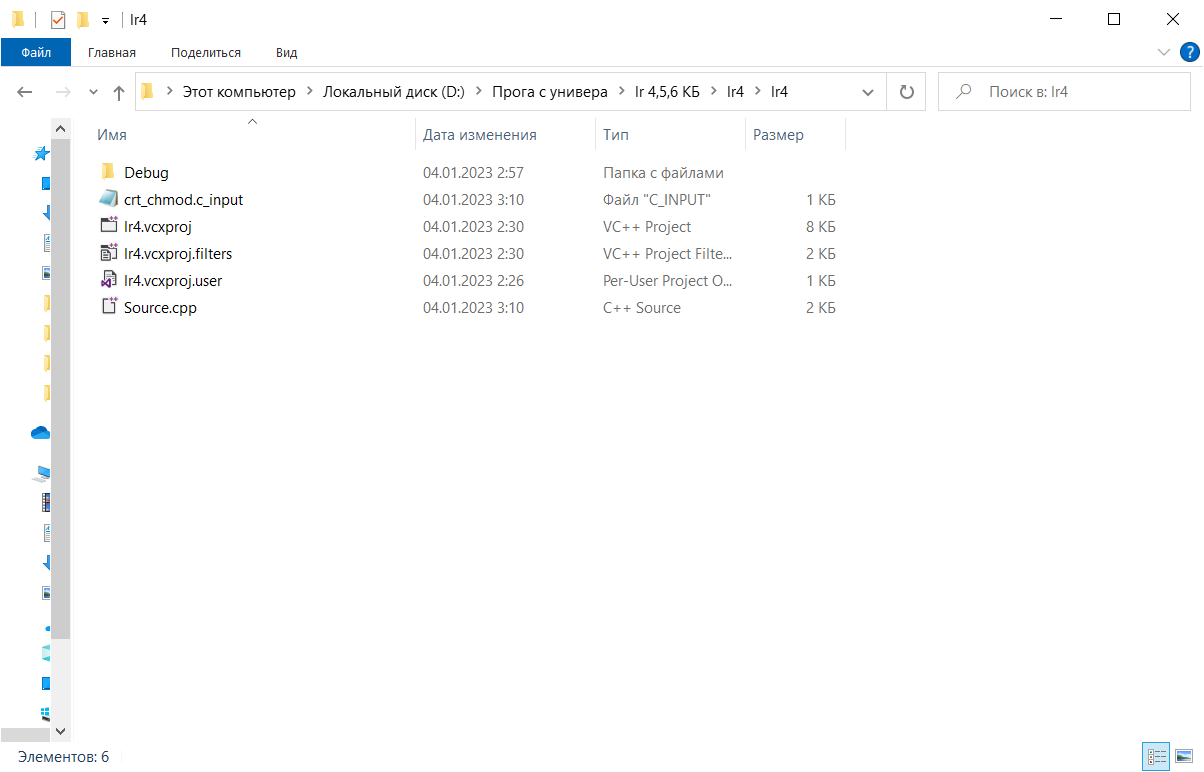
1) Папка до запуску програми:



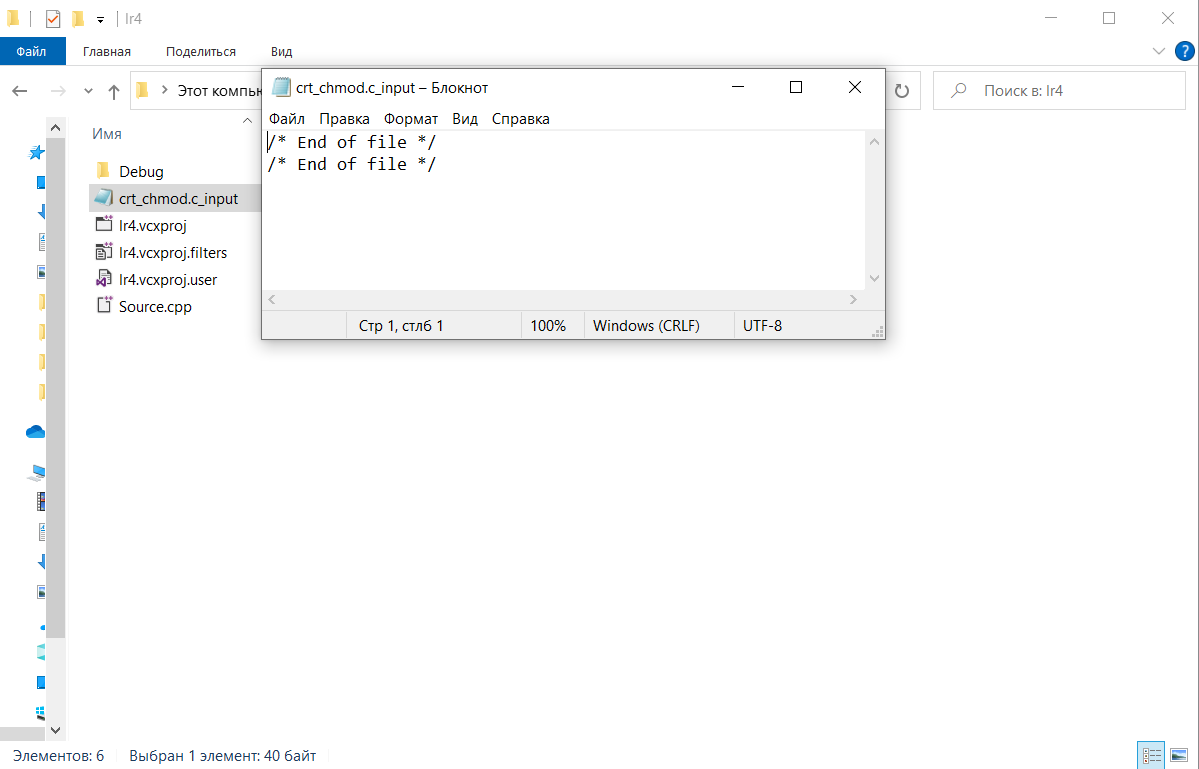
2) Папка після запуску програми:



3) Спроба записати нову інформацію у файл



4) Вміст файлу:



Як бачимо, відкрити файл та записати в нього інформацію вдалось тільки 2 рази, хоча спроби було 3. Це сталося, тому що при одній зі спроб читання та запис у файл були заборонені. Одже програма вірно виконує поставлену задачу.

**Висновок**: для змін прав доступу для різних користувачів системи можна використати списки контролю доступу Access-Contol List. Це потрібно для того, щоб дозволити або обмежити дії певної групи користувачів з конкретним файлом.