1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 1**

1. «Настройки безопасности пользователей в ОС Windows»
2. по дисциплине «Безопасность современных информационных технологий»
3. Выполнил
4. студент гр. 4851003/00802 Вологдин М.В.

<*подпись*>

1. Преподаватель Соловей Р.С.

<*подпись*>

1. Санкт-Петербург
2. 2023
3. **Цель работы**

Изучить существующие настройки безопасности пользователейв ОС Windowsи возможности управления пользователями с использованием WindowsAPI.

1. **Задача**

Реализовать программу для управления учетными записями и контролем доступа в ОС Windows, использующую возможности WindowsAPI.

Требования:

* язык программирования: C/C++;
* динамическая подгрузка библиотек Windows, реализующих функции Windows API;
* разрабатываемая программа не должна использовать готовые обертки над Windows API;
* программа должна выводить списки зарегистрированных в системе пользователей и групп, их SID и привилегии;
* программа должна позволять добавлять/изменять/удалять пользователей и группыв ОС, а также удалять и добавлять, включать и выключать им привилегии;
* программа должнав ОС Windows 7–10.

1. **Ход работы**

Для реализации программы были динамически подключены библиотеки Advapi32 и netapi32. С помощью этих библиотек были добавлены функции, которые можно увидеть на рисунке 1.

Изображение выглядит как текст, табличка

Автоматически созданное описание

Рисунок 1 – Определение функций из динамических библиотек

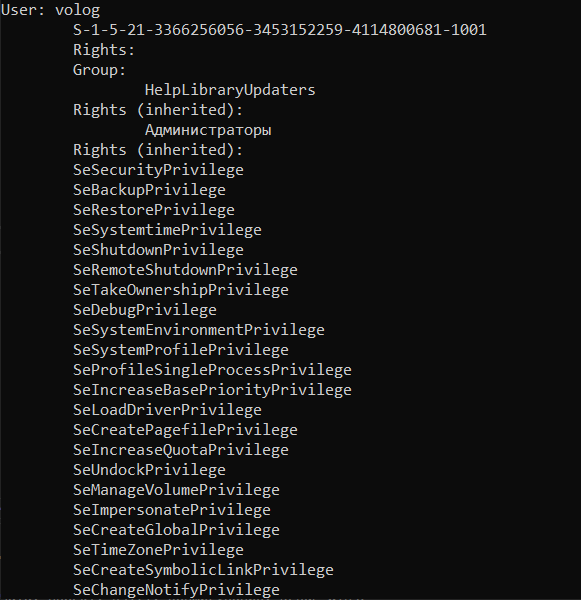
Программа позволяет выводить на экран информацию о пользователях, группах пользователей, добавлять и удалять пользователей и группы пользователей, добавлять и удалять привилегии для пользователей и групп, а также добавлять и удалять пользователей из группы. Меню можно увидеть на рисунке 2.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2 – Меню программы

Формат вывода информации таков: сначала выводится SID пользователя/группы, после чего выводятся его права, список групп, к которым принадлежит пользователь, и его права, наследуемые от групп (рисунок 3).



1. **Контрольные вопросы**

1. Для чего нужны и как работают привилегии «Взятие во владение», «Архивирование файлов и каталогов», «Восстановление файлов и каталогов»? –

* «Взятие во владение» (SeTakeOwnershipPrivilege) – требуется для приобретения прав владения объектом без предоставления избирательного доступа;
* «Архивирование файлов и каталогов» (SeBackupPrivilege) – заставляет NTFS предоставить следующие виды доступа к любому файлу или каталогу, не обращая внимание на имеющийся дескриптор безопасности:
* READ\_CONTROL – право чтения информации об объекте в его дескрипторе безопасности за исключением SACL;
* ACCESS\_SYSTEM\_SECURITY – право чтения и изменения SACL объекта;
* FILE\_GENERIC\_READ – право доступа на чтение;
* FILE\_TRAVERSE – право проходить каталог;
* «Восстановление файлов и каталогов» (SeRestorePrivilege) – Эта привилегия заставляет NTFS предоставлять следующие виды доступа любому файлу или каталогу, независимо от имеющегося дескриптора безопасности:
* WRITE\_DAC – право изменять DACL объекта;
* WRITE\_OWNER – право менять владельца объекта;
* ACCESS\_SYSTEM\_SECURITY – право чтения и изменения SACL объекта;
* FILE\_GENERIC\_WRITE – право доступа для записи в файл;
* FILE\_ADD\_FILE – право на запись данных в файл (или создания файла в директории);
* FILE\_ADD\_SUBDIRECTORY – на добавление данных в файл (или создания подкаталога в директории);
* DELETE – право на удаление объекта.

2. Какой привилегией в системе должен обладать пользователь для того, чтобы он мог выполять отладку процессов? –

Для того, чтобы пользователь мог выполнять отладку процессов, ему требуется привилегия SeDebugPrivilege.

3. Какие еще факторы (кроме прав доступа, привилегий, владельца) влияют на доступ субъектов к объектам в ОС Windows? –

На доступ субъектов к объектам в ОС Windows помимо основных факторов влияют:

* действующая политика безопасности.

4. Почему учетная запись Гостя обычно отключена по умолчанию? –

Учетная запись Гостя позволяет случайным или разовым пользователям, не имеющим учетную запись на комьютере, производить временный вход на локальный сервер или клиентский компьютер с ограниченными правами. К тому же данная учетная запись имеет пустой пароль. Учитывая, что учетной записи можно предоставить анонимный доступ, существует риск для безопасности системы. По этой причине учетная запись Гостя обычно отключена по умолчанию.

5. Что такое RID? –

RID (Relative Identifier) – относительный идентификатор – это число переменной длины, которое присваивается объекту при создании и становится частью его SID, однозначно идентифицирующее учетную запись или группу в домене.

1. **Выводы**

В ходе работы было изучено ещё одно применение WIN API - работа с пользователями, группами и привилегиями. Также реализована программа, выполняющая функции управления учётными записями Windows.