МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

ЛАБОРАТОРНАЯ РАБОТА №7

ОТЧЁТ

студента 2 курса 251 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Григорьева Данилы Евгеньевича

Проверено:

Старший преподаватель _____ Е. М. Черноусова

Саратов 2024

СОДЕРЖАНИЕ

1 Текст программы на языке ассемблера с комментариями

```
extrn GetUserNameW : proc, GetComputerNameW : proc, GetTempPathW :
proc, wsprintfW : proc, MessageBoxW : proc, ExitProcess : proc,
RegGetValueW : proc

szMAX_COMP_NAME   = 16
szULEN            = 256
szMAX_PATH        = 261 ;262
szREVISION_NUMBER = 64
ERROR_SUCCESS     = 0
NULL              = 0
RRF_RT_REG_SZ     = 2


.data
    ; UTF-16le "Информация о системе"
    caption  db 18h, 04h, 3dh, 04h, 44h, 04h, 3eh, 04h, 40h, 04h,
3ch, 04h, 30h, 04h, 46h, 04h, 38h, 04h, 4fh, 04h, 20h, 00h, 3eh,
04h, 20h, 00h, 41h, 04h, 38h, 04h
             db 41h, 04h, 42h, 04h, 35h, 04h, 3ch, 04h, 35h, 04h,
00h, 00h
    ; UTF-16le $'Пользователь: %s\r\nКомпьютер: %s\r\nВременная
папка: %s\nВерсия ОС: %s\n'
    message  db 1fh, 04h, 3eh, 04h, 3bh, 04h, 4ch, 04h, 37h, 04h,
3eh, 04h, 32h, 04h, 30h, 04h, 42h, 04h, 35h, 04h, 3bh, 04h, 4ch,
04h, 3ah, 00h, 20h, 00h, 25h, 00h
             db 73h, 00h, 0dh, 00h, 0ah, 00h, 1ah, 04h, 3eh, 04h,
3ch, 04h, 3fh, 04h, 4ch, 04h, 4eh, 04h, 42h, 04h, 35h, 04h, 40h,
04h, 3ah, 00h, 20h, 00h, 25h, 00h
             db 73h, 00h, 0dh, 00h, 0ah, 00h, 12h, 04h, 40h, 04h,
35h, 04h, 3ch, 04h, 35h, 04h, 3dh, 04h, 3dh, 04h, 30h, 04h, 4fh,
04h, 20h, 00h, 3fh, 04h, 30h, 04h
             db 3fh, 04h, 3ah, 04h, 30h, 04h, 3ah, 00h, 20h, 00h,
25h, 00h, 73h, 00h, 0ah, 00h
             db 12h, 04h, 35h, 04h, 40h, 04h, 41h, 04h, 38h, 04h,
4fh, 04h, 20h, 00h, 1eh, 04h, 21h, 04h, 3ah, 00h, 20h, 00h, 25h,
00h, 73h, 00h, 0ah, 00h, 0ah, 00h
             db 00h, 00h
    ; UTF-16le "Ошибка"
    error    db 1eh, 04h, 48h, 04h, 38h, 04h, 31h, 04h, 3ah, 04h,
30h, 04h
             db 00h, 00h
    ; UTF-16le "Не могу прочитать имя пользователя"
    erUser   db 1dh, 04h, 35h, 04h, 20h, 00h, 3ch, 04h, 3eh, 04h,
```

```
33h, 04h, 43h, 04h, 20h, 00h, 3fh, 04h, 40h, 04h, 3eh, 04h, 47h,
04h, 38h, 04h, 42h, 04h, 30h, 04h
            db 42h, 04h, 4ch, 04h, 20h, 00h, 38h, 04h, 3ch, 04h,
4fh, 04h, 20h, 00h, 3fh, 04h, 3eh, 04h, 3bh, 04h, 4ch, 04h, 37h,
04h, 3eh, 04h, 32h, 04h, 30h, 04h
            db 42h, 04h, 35h, 04h, 3bh, 04h, 4fh, 04h, 0ah, 00h
            db 00h, 00h
    ; UTF-16le "Не могу прочитать имя компьютера"
    erComp   db 1dh, 04h, 35h, 04h, 20h, 00h, 3ch, 04h, 3eh, 04h,
33h, 04h, 43h, 04h, 20h, 00h, 3fh, 04h, 40h, 04h, 3eh, 04h, 47h,
04h, 38h, 04h, 42h, 04h, 30h, 04h
            db 42h, 04h, 4ch, 04h, 20h, 00h, 38h, 04h, 3ch, 04h,
4fh, 04h, 20h, 00h, 3ah, 04h, 3eh, 04h, 3ch, 04h, 3fh, 04h, 4ch,
04h, 4eh, 04h, 42h, 04h, 35h, 04h
            db 40h, 04h, 30h, 04h, 0ah, 00h
            db 00h, 00h
    ; UTF-16le "Не могу найти папку временного хранилища"
    erTemp   db 1dh, 04h, 35h, 04h, 20h, 00h, 3ch, 04h, 3eh, 04h,
33h, 04h, 43h, 04h, 20h, 00h, 3dh, 04h, 30h, 04h, 39h, 04h, 42h,
04h, 38h, 04h, 20h, 00h, 3fh, 04h
            db 30h, 04h, 3fh, 04h, 3ah, 04h, 43h, 04h, 20h, 00h,
32h, 04h, 40h, 04h, 35h, 04h, 3ch, 04h, 35h, 04h, 3dh, 04h, 3dh,
04h, 3eh, 04h, 33h, 04h, 3eh, 04h
            db 20h, 00h, 45h, 04h, 40h, 04h, 30h, 04h, 3dh, 04h,
38h, 04h, 3bh, 04h, 38h, 04h, 49h, 04h, 30h, 04h, 0ah, 00h
            db 00h, 00h
    ; UTF-16le "Не могу получить версию Windows"
    erWinver db 1dh, 04h, 35h, 04h, 20h, 00h, 3ch, 04h, 3eh, 04h,
33h, 04h, 43h, 04h, 20h, 00h, 3fh, 04h, 3eh, 04h, 3bh, 04h, 43h,
04h, 47h, 04h, 38h, 04h, 42h, 04h
            db 4ch, 04h, 20h, 00h, 32h, 04h, 35h, 04h, 40h, 04h,
41h, 04h, 38h, 04h, 4eh, 04h, 20h, 00h, 57h, 00h, 69h, 00h, 6eh,
00h, 64h, 00h, 6fh, 00h, 77h, 00h
            db 73h, 00h, 0ah, 00h
            db 00h, 00h
    ; UTF-16le $'Software\\Microsoft\\Windows NT' (prefix)
    regPath  db 53h, 00h, 6fh, 00h, 66h, 00h, 74h, 00h, 77h, 00h,
61h, 00h, 72h, 00h, 65h, 00h, 5ch, 00h, 4dh, 00h, 69h, 00h, 63h,
00h, 72h, 00h, 6fh, 00h, 73h, 00h
            db 6fh, 00h, 66h, 00h, 74h, 00h, 5ch, 00h, 57h, 00h,
69h, 00h, 6eh, 00h, 64h, 00h, 6fh, 00h, 77h, 00h, 73h, 00h, 20h,
00h, 4eh, 00h, 54h, 00h, 5ch, 00h
    ; UTF-16le CurrentVersion
    regKey   db 43h, 00h, 75h, 00h, 72h, 00h, 72h, 00h, 65h, 00h,
```

```
6eh, 00h, 74h, 00h, 56h, 00h, 65h, 00h, 72h, 00h, 73h, 00h, 69h,
00h, 6fh, 00h, 6eh, 00h
            db 00h, 00h
    ; HKEY_LOCAL_MACHINE
    hKey     dd 80000002h
    ; MB_ICONERROR | MB_OK
    errFlags dd 00000010h

    ; Длинные строковые переменные не локальные, чтобы избежать
переполнения стека
    msg      dw 512 dup (0)
    username dw szULEN dup (0)
    compname dw szMAX_COMP_NAME dup (0)
    temppath dw szMAX_PATH dup (0)
    version  dw szREVISION_NUMBER dup (0)

.code
Halt proc
    sub rsp, 8
    mov rdx, rcx
    xor rcx, rcx
    lea r8, error
    xor r9, r9
    call MessageBoxW
    xor rcx, rcx
    call ExitProcess
    add rsp, 8
Halt endp
mainCRTStartup proc
    local _size:dword
    push rbp

    mov _size, szULEN
    lea rcx, username
    lea rdx, _size
    call GetUserNameW
    jnz get_compname
        lea rcx, erUser
        call Halt

    get_compname:
    mov _size, szMAX_COMP_NAME
    lea rcx, compname
    lea rdx, _size
```

```
call GetComputerNameW
jnz get_temppath
    lea rcx, erComp
    call Halt

get_temppath:
mov _size, szMAX_PATH
lea rdx, temppath
;lea rcx, _size
mov rcx, szMAX_PATH
call GetTempPathW
jnz get_winver
    lea rcx, erTemp
    call Halt

get_winver:
sub rsp, 30h
mov _size, szREVISION_NUMBER
lea rax, _size
mov [rsp+30h],rax
lea rax,version
mov [rsp+28h],rax
xor rax, rax
mov [rsp+20h],rax
mov r9d, RRF_RT_REG_SZ
lea r8, regKey
lea rdx, regPath
mov rcx,0FFFFFFFF80000002h ; hKey
call RegGetValueW
test eax,eax
je output
    lea rcx, erWinver
    call Halt

output:
sub rsp, 30h
lea rcx, version; _temppath
mov [rsp + 28h], rcx
lea rcx, temppath; _temppath
mov [rsp + 20h], rcx
lea rcx, msg
lea rdx, message
lea r8, username
lea r9, compname
```

```
    call wsprintfW

    xor RCX, RCX
    lea RDX, msg
    lea R8, caption
    xor R9, R9
    call MessageBoxW
    xor RCX, RCX
    call ExitProcess
    pop rbp
    ret
mainCRTStartup endp
end
```

2 Скриншот запуска программы