**Міністерство освіти і науки України**

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Факультет інформатики та обчислювальної техніки**

**Кафедра обчислювальної техніки**

**Лабораторна робота № 2**

з дисципліни

«Системне програмування»

на тему

“Дослідження структури програм у форматі COM”

Виконав:

Перевірив:

студент групи ІП-93 доцент

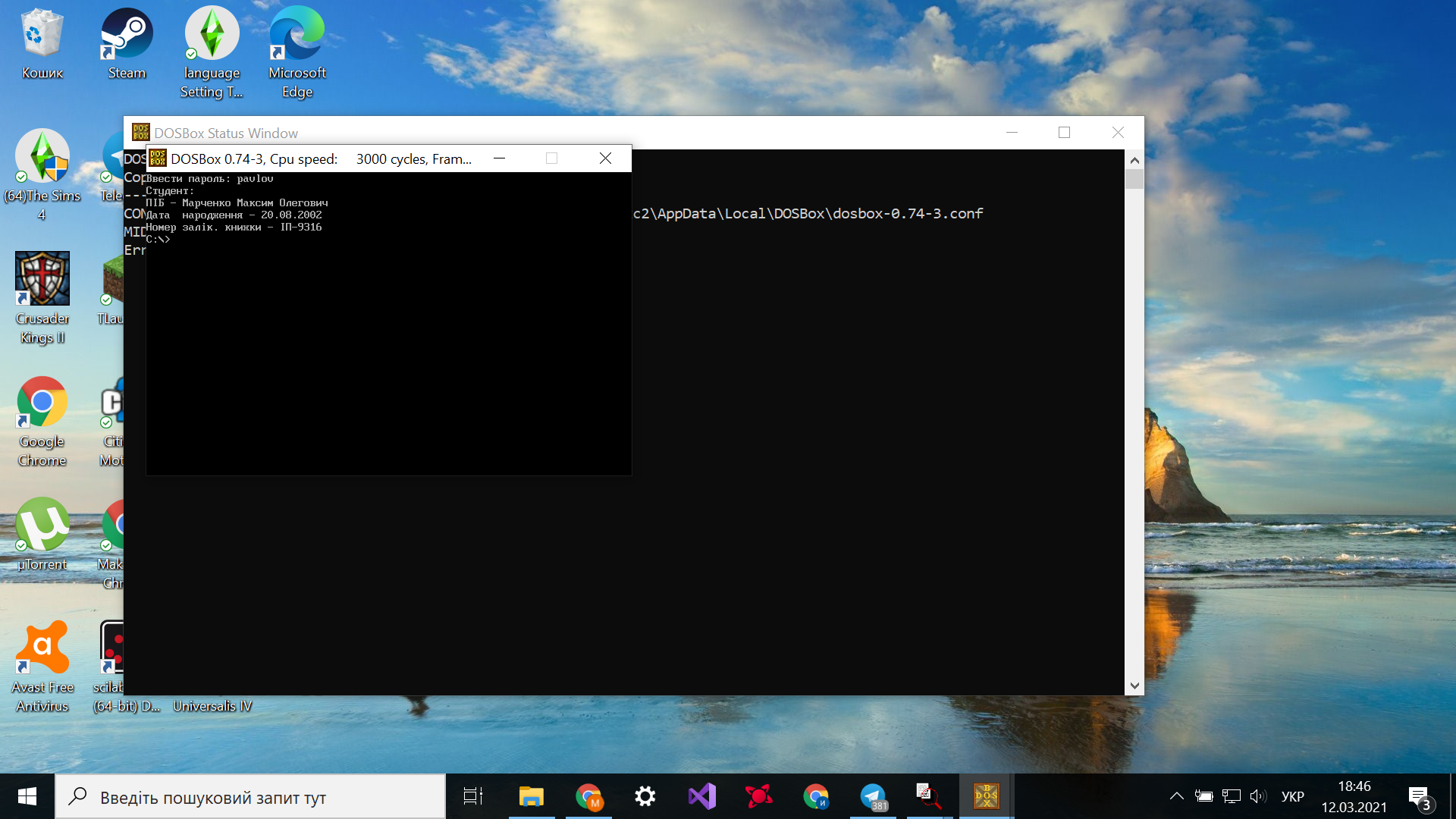
Марченко Максим Олегович Павлов В.Г.

номер залікової книжки: 9316

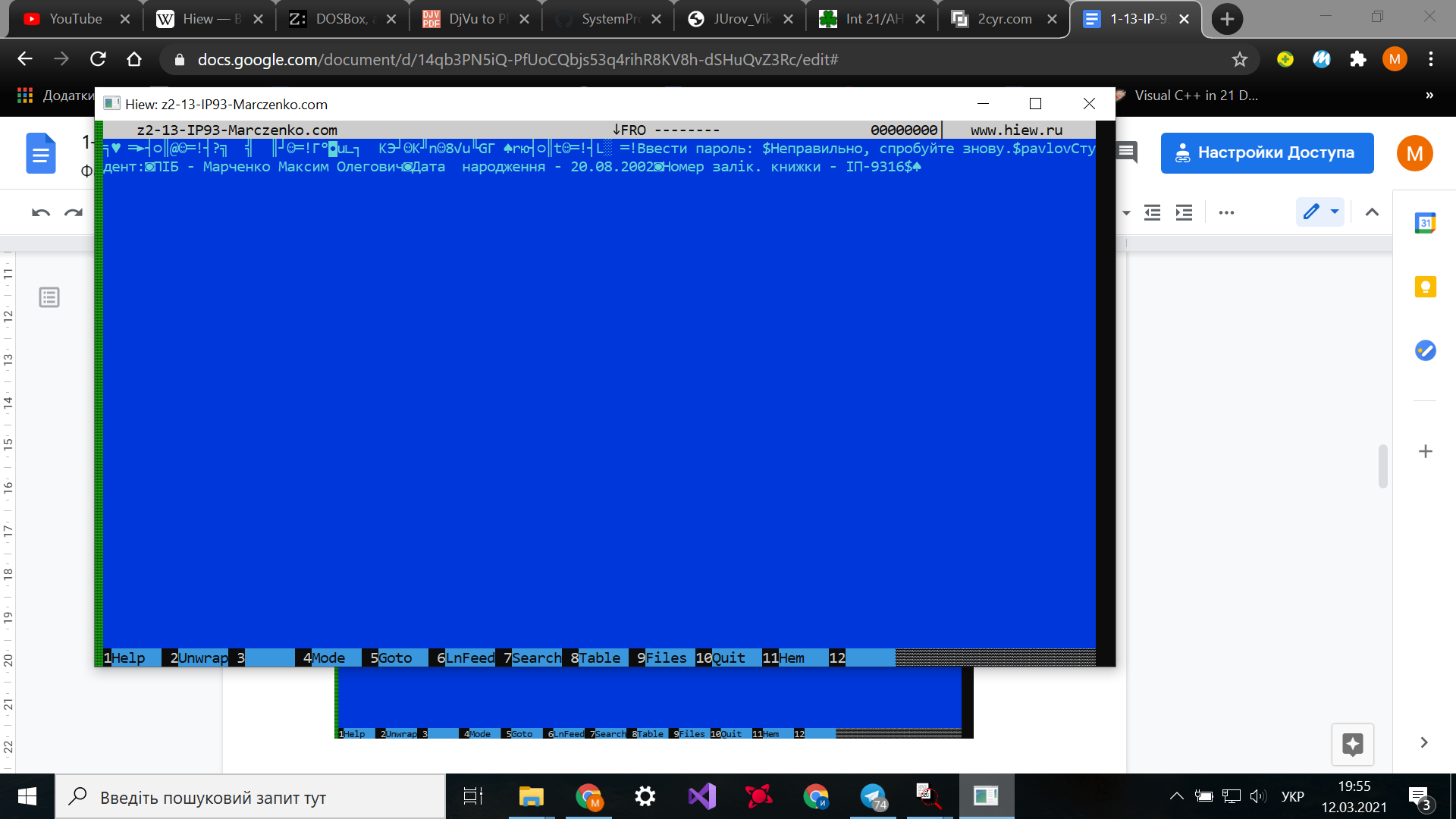
Київ 2020

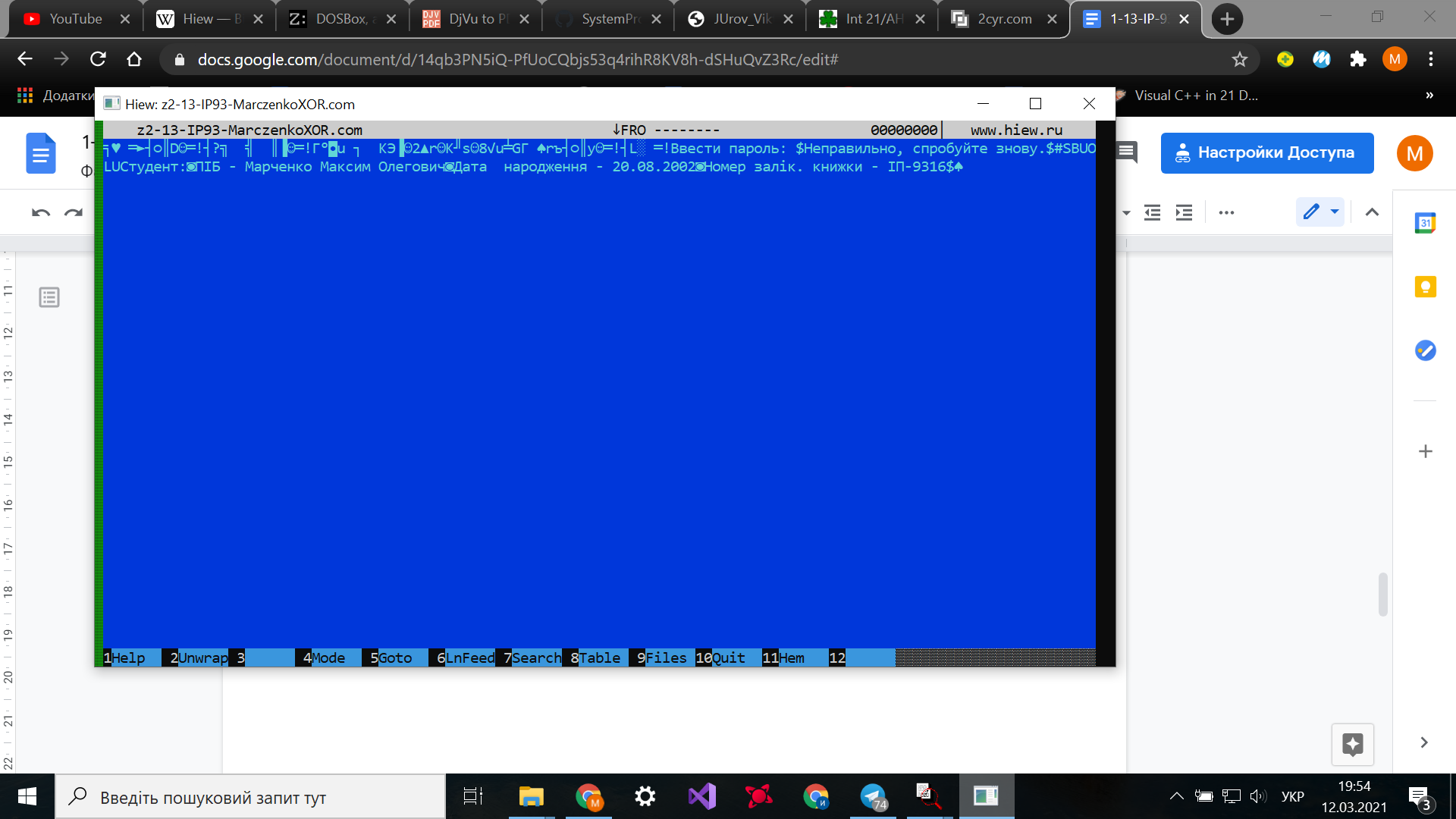
Скріншот виконання

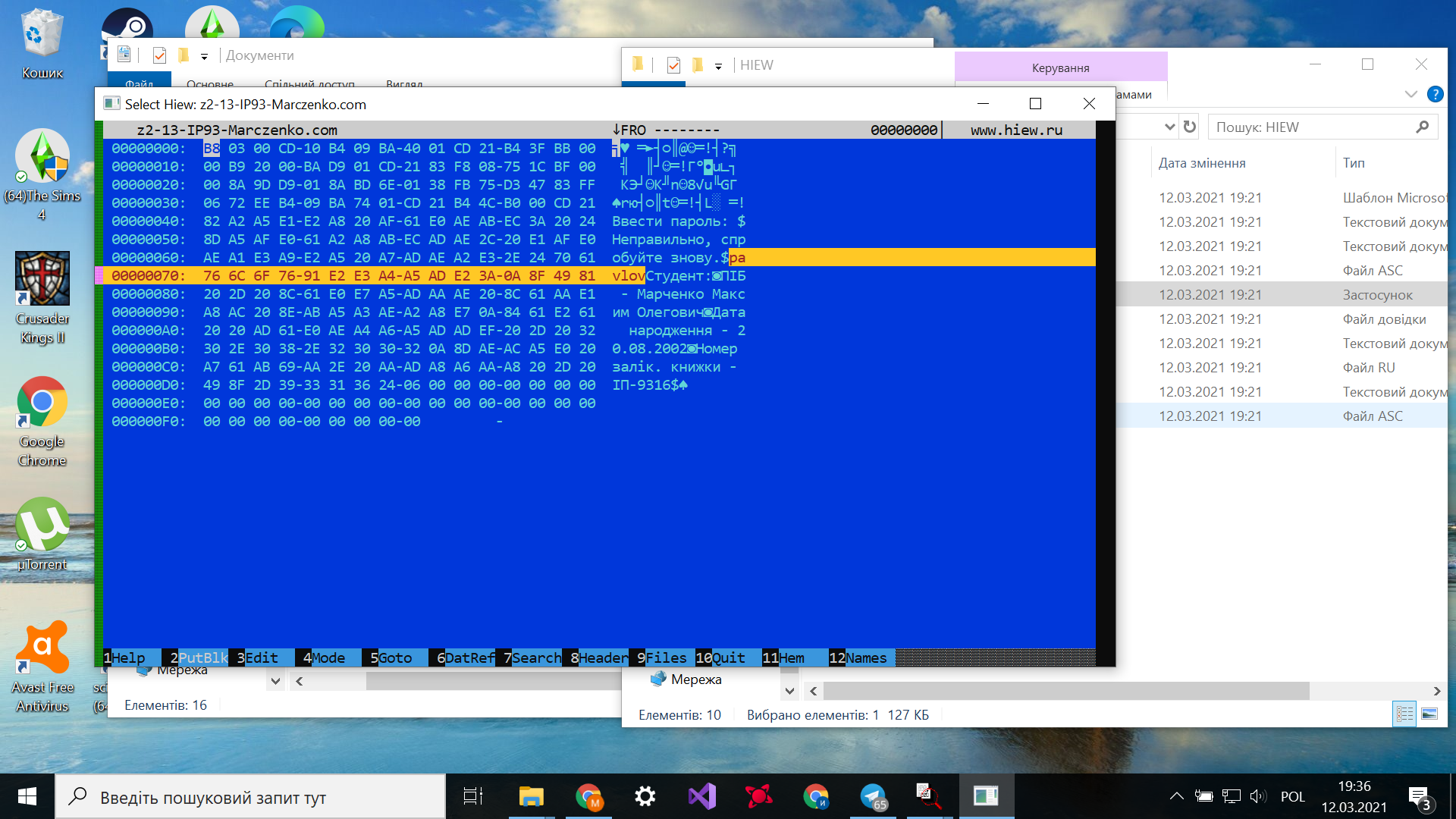
Для виконання програм формату .com потрібне спеціальне програмне забезпечення, у цьому випадку було використано DOSBox. Для того, щоб уможливити коректне відображення кириличних символів, перед запуском файлу, у досбокс було запущено команду keyb none 866, що встановлює дане кодування.

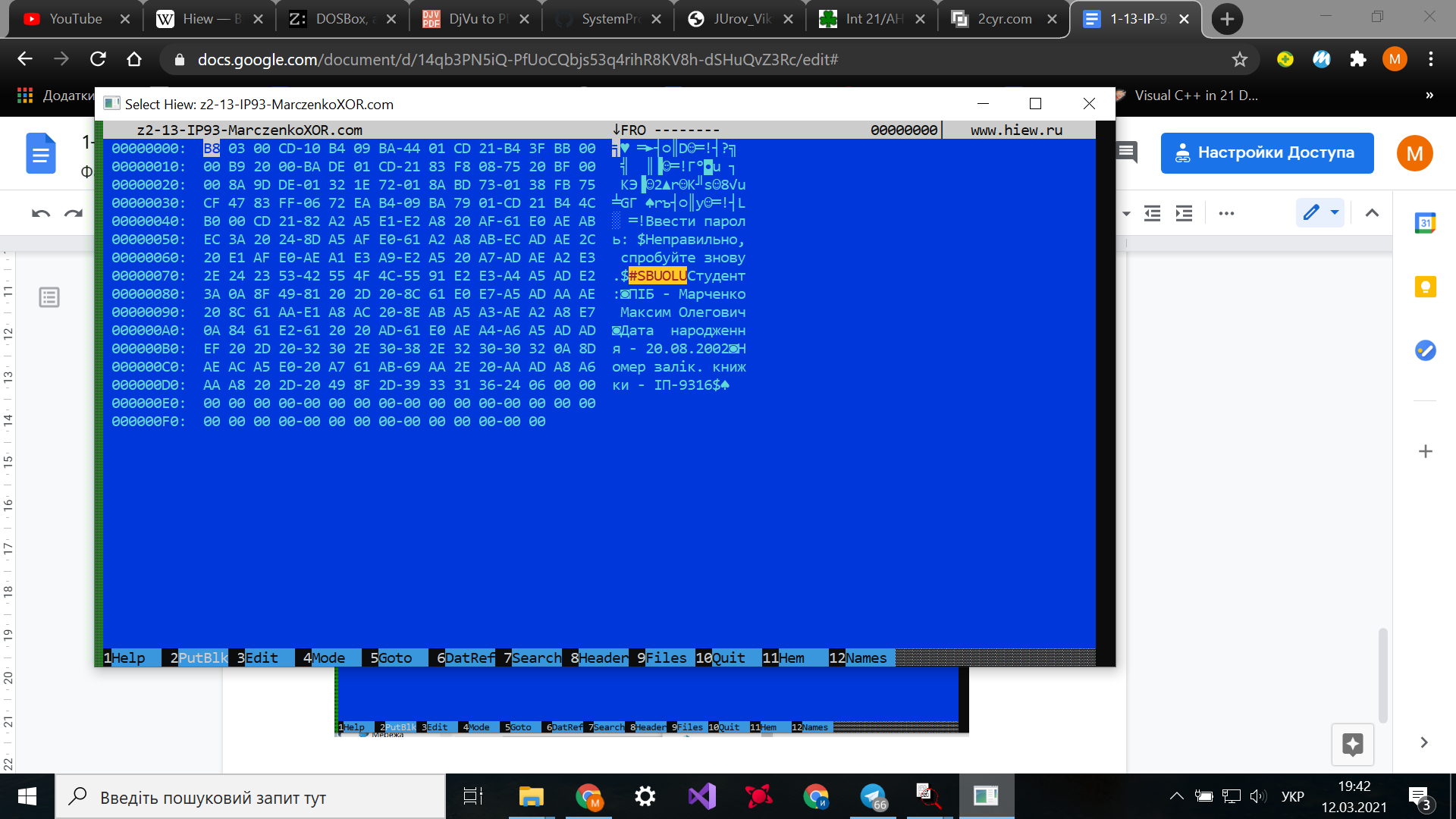


Обидві програми мають однаковий вигляд при виконанні, відмінності між ними є лише в тому, як вони зберігають паролі. Перевірити це можемо, відкривши відповідні файли розширення .com y HIEW. (В якості паролю використовувався рядок “pavlov”)







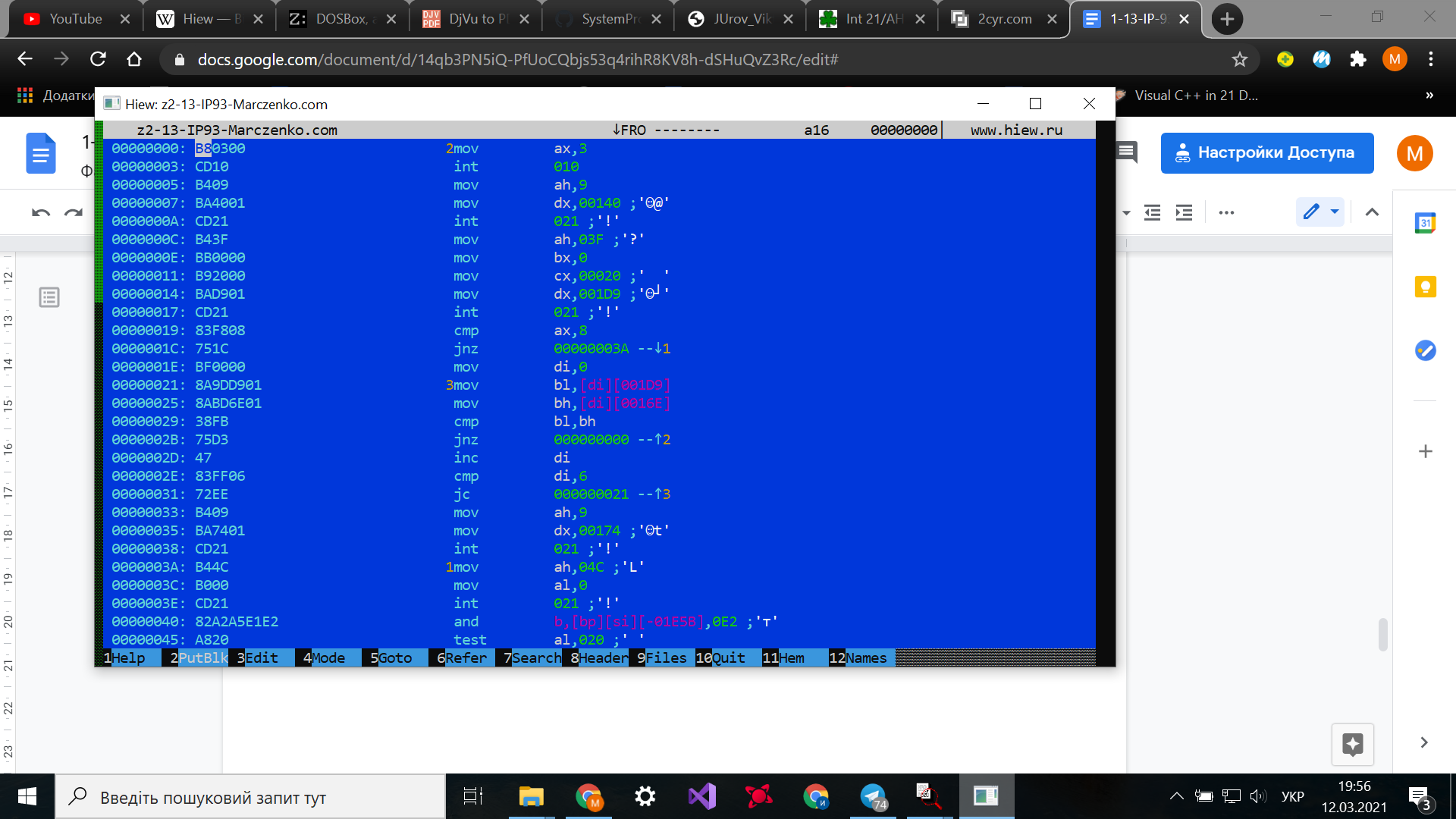


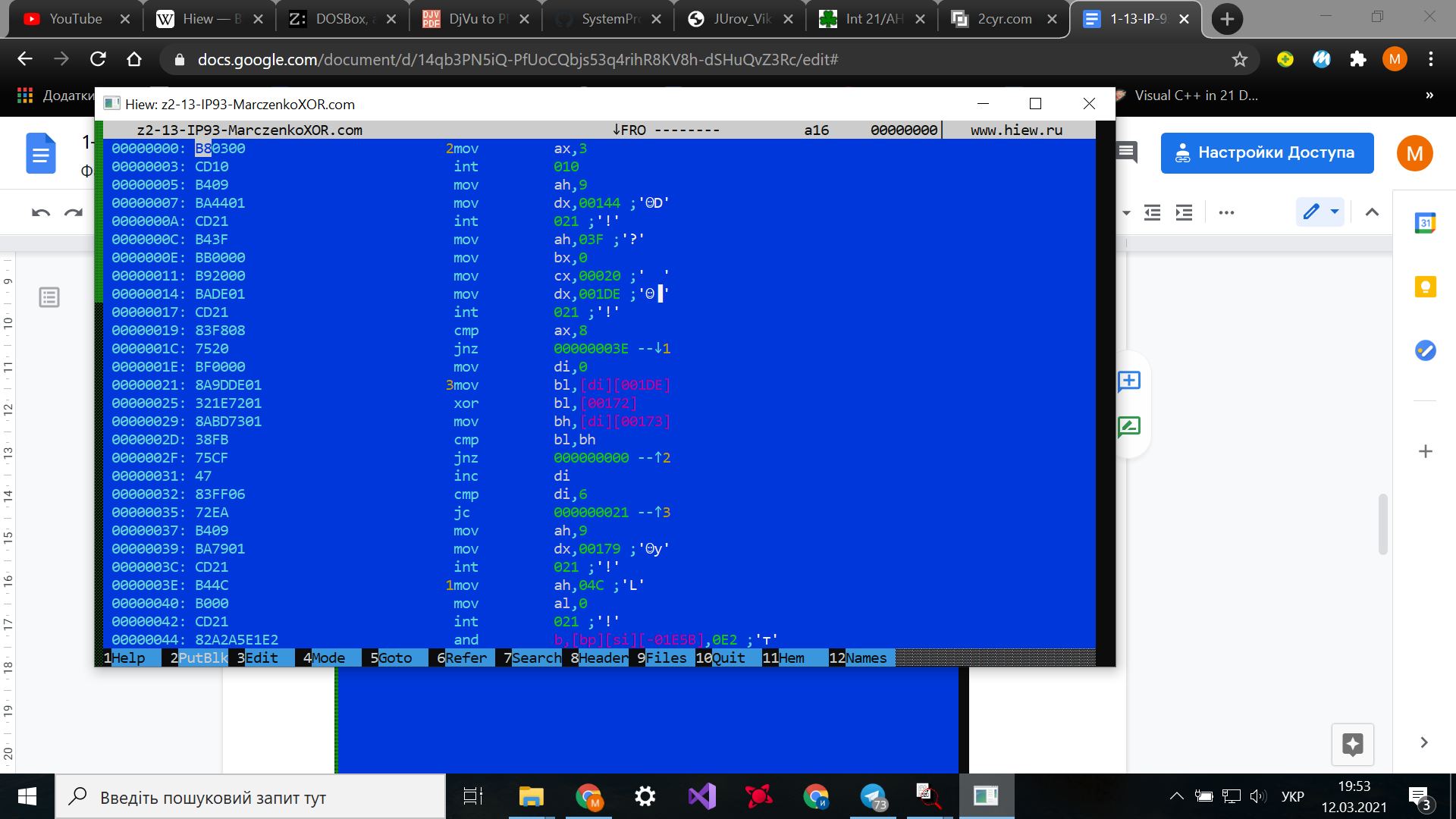
Незважаючи на те, що пароль, що потрібно ввести користувачеві у обох випадках був однаковий, у другій версії програми його немає, оскільки застосовувалося шифрування методою ХОR. Шифрування відбувається таким способом:

1. Рядок розбивається на окремі літери, котрі через систему ASCII переводяться у двійкове число
2. Для кожного біту цього восьмизначного числа, застосовуємо бінарну операцію “виключне або” з певним числом (у моєму випадку це число 23h).
3. Знайдені біти конкатинуються у восьмибітне число, яке за системою ASCII переводиться у символ.
4. Всі знайдені символи конкатинуються в один рядок, який і зберігається у програмі (рядок SBUOLU).

Для дешифрування повторюємо той самий алгоритм, на вході подаємо вже зашифровану версію рядка.

Даний спосіб шифрування є одним з найпростіших як для імплементації, так і для дешифрування чи взлому, проте він захищає дані краще, ніж взагалі не застосовувати жодного шифрування, як помітно зі скриншотів.





При порівнянні коду з Debug та вихідного коду файлу розширення .asm, видно, що після дебаггингу у програмі є лише команди, без початкових даних, чи структурування.

Розглянемо команди MOV:

|  |  |  |
| --- | --- | --- |
| Команда | Операнд | КОП |
| mov ax, 3 | 03 | BB |
| mov ah, 9 | 09 | B4 |
| mov dx, 00144 | 44 01 | Ba |
| mov ah, 03F | 3F 00 | B4 |
| mov bx, 0 | 00 | BB |
| mov cx, 00020 | 20 00 00 | B9 |
| mov dx, 001DE | DE 01 | BA |
| mov di, 0 | 00 | BF |
| mov dx, 00179 | 79 01 | BA |
| mov ah, 04C | 4C 00 | B4 |
| mov al, 0 | 00 | B0 |

Висновки: Впродовж виконання даної лабораторної роботи було ознайомлено з структурою файлів .com - простий тип виконуваного файлу, що застосовувався у операційній системі DOS. У COM-програмах використовується модель пам'яті tiny, а сирцевий код, початкові дані та стек розташовуються в одному сегменті. Отримані файли цього формату мають відмінності від файлів типу .asm, зокрема тим, не структурують дані, та є по суті просто списком системних команд. Також було розібрано будову команд mov, та ознайомлено з шифруванням методою XOR, створення та запуск batch-

Додаток: Код програми 2-13-IP93-MarczenkoXOR

.model tiny

.data

START\_MSG DB "‚ўҐбвЁ Їaа®«м: $"

ERROR\_MSG DB "ЌҐЇаaўЁ«м­®, бЇа®Ўг©вҐ §­®ўг.$"

PASSWD\_KEY DB 23h

PASSWD DB "SBUOLU"

DATA DB "‘вг¤Ґ­в:", 10,

"ЏIЃ - ЊaазҐ­Є® ЊaЄбЁ¬ Ћ«ҐЈ®ўЁз", 10,

"„aвa ­aа®¤¦Ґ­­п - 20.08.2002", 10,

"Ќ®¬Ґа §a«iЄ. Є­Ё¦ЄЁ - IЏ-9316$"

PASSWD\_LEN DB 6

USR\_INPUT DB 32 DUP (?)

.code

org 100h

.startup

MAIN:

MOV AX, 03h

INT 10h

MOV AH, 09h

MOV DX, offset START\_MSG

INT 21h

MOV AH, 3Fh

MOV BX, 0

MOV CX, 32

MOV DX, offset USR\_INPUT

INT 21h

CMP AX, 8

JNE EXIT

MOV DI, 0

VALIDATION:

MOV BL, USR\_INPUT[DI]

XOR BL, PASSWD\_KEY

MOV BH, PASSWD[DI]

CMP BL, BH

JNE MAIN

INC DI

CMP DI, 6

JB VALIDATION

MOV AH, 09h

MOV DX, offset DATA

INT 21h

EXIT:

MOV AH, 4Ch

MOV AL, 0

INT 21h

END