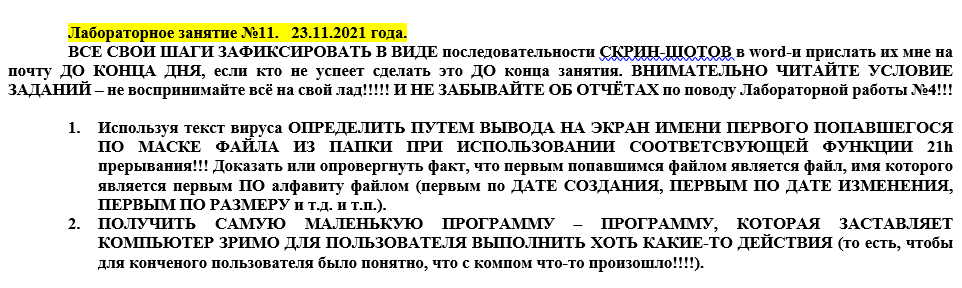
Жуковский Павел Сергеевич, 4 курс, 12 группа

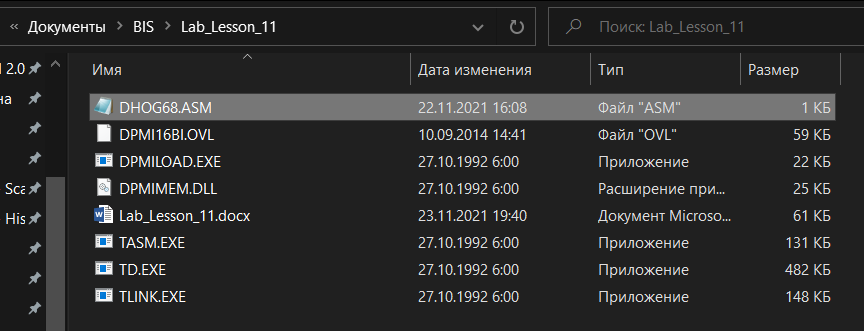
Лабораторное занятие №11

Пароль от архива: **041**

Постановка задачи:

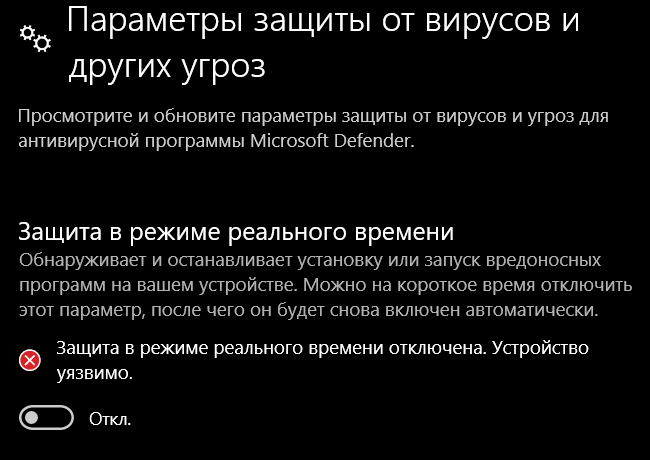
Алгоритм решения:

Для начала возьмём исходный текст вируса, предложенный в лекции, и поместим в файл **DHOG68.ASM**:



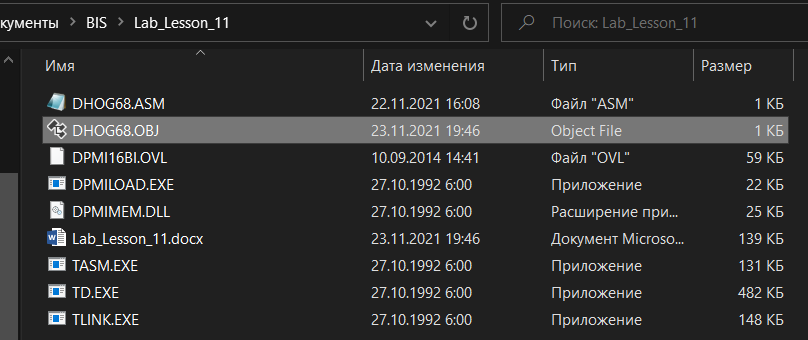
Помимо исходного текста я также переместил в текущую папку несколько полезных исполняемых модулей, которые мы часто используем для получения своих объектных и исполнимых модулей.

Так как мы имеем дело с вирусом, то я сразу отключил свой антивирус, чтобы он не мешал экспериментам:

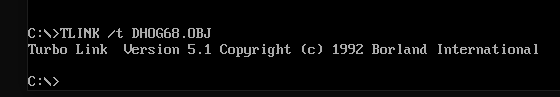


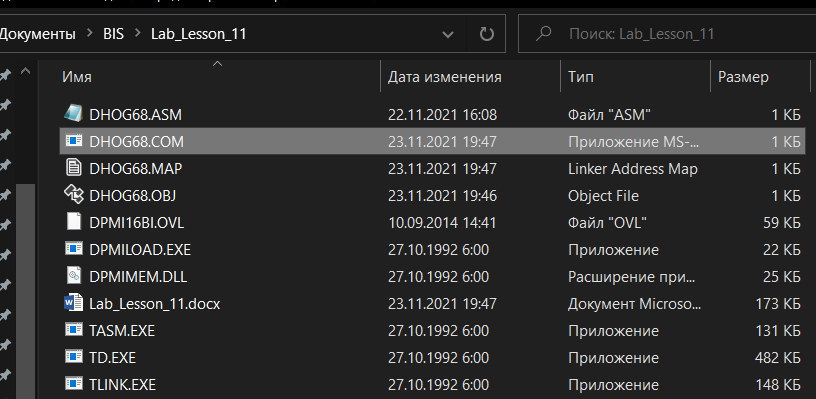
Теперь получим объектный модуль **DHOG68.OBJ**:





Затем получим исполнимый модуль **DHOG68.COM**:

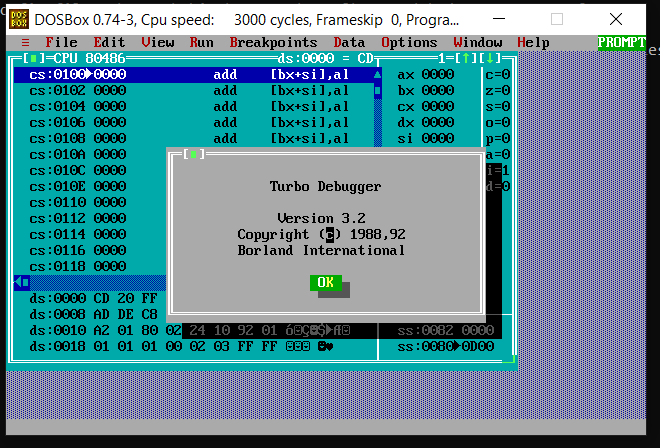




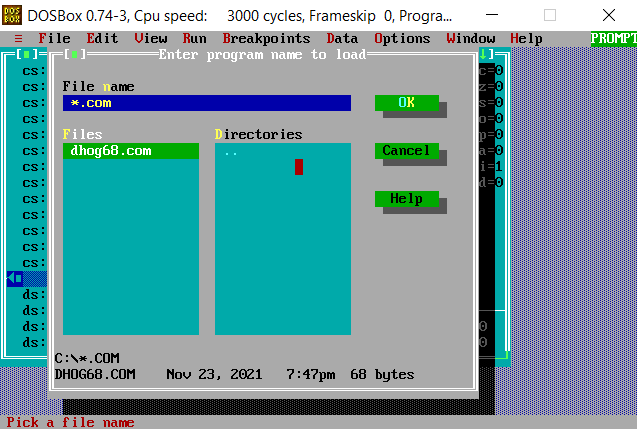
Далее, я создал копию всех файлов текущей директории, чтобы не потерять их в случае, если что-то пойдёт не так (включая этот отчёт).

Теперь мы готовы к эксперименту.

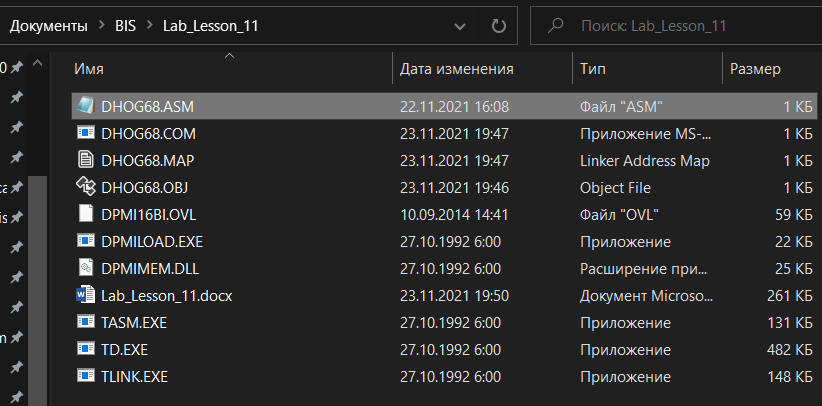
Запускаем отладчик **TD.EXE**:



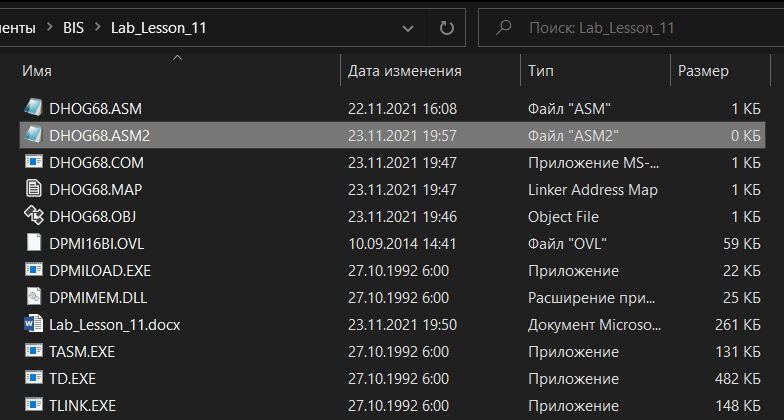
И загружаем в него программу вируса:



Самым первым файлом (в лексикографическом порядке) выступает файл с исходным текстом:



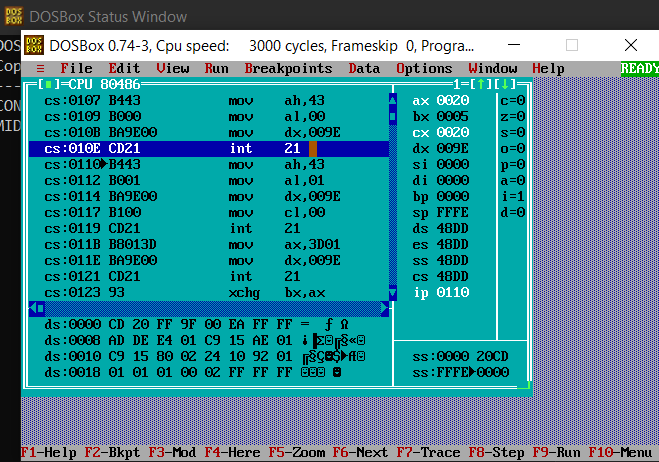
Поэтому создадим ещё один (пустой) файл с именем **DHOG68.ASM2**:



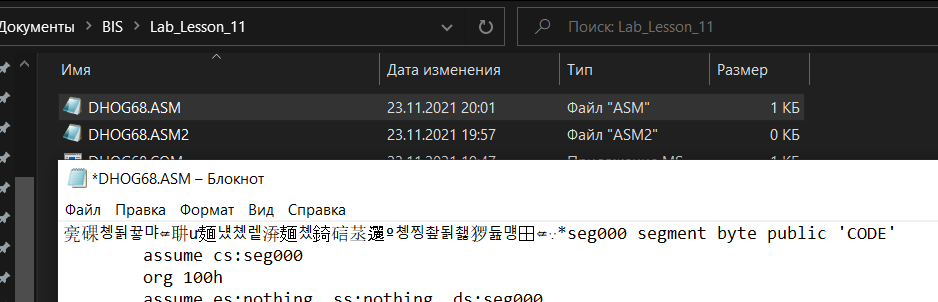
Теперь будем постепенно проходить отладчиком по программе вируса и следить за тем, какой из этих файлов заразиться раньше.

Файл **DHOG68.ASM –** первый в лексикографическом порядке, а файл **DHOG68.ASM2 –** самый маленький по размеру. Результатом эксперимента мы узнаем, кто из них заразится вирусными машинными инструкциями в первую очередь.

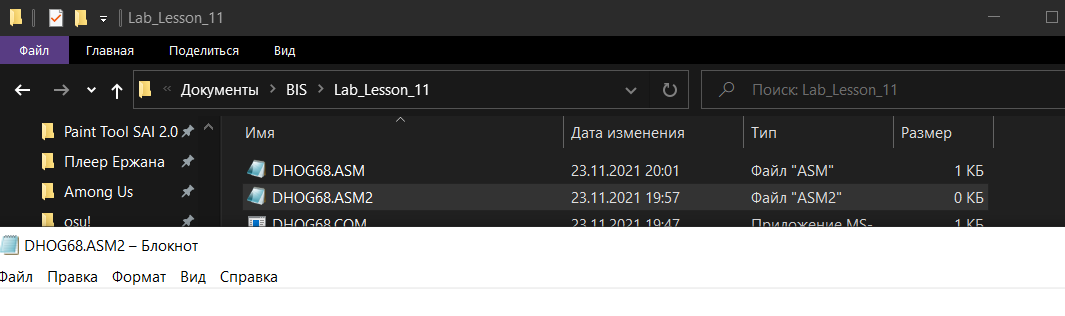
На данном шаге программы вируса я решил остановиться:



Я проверил исходные файлы, сначала **DHOG68.ASM**:

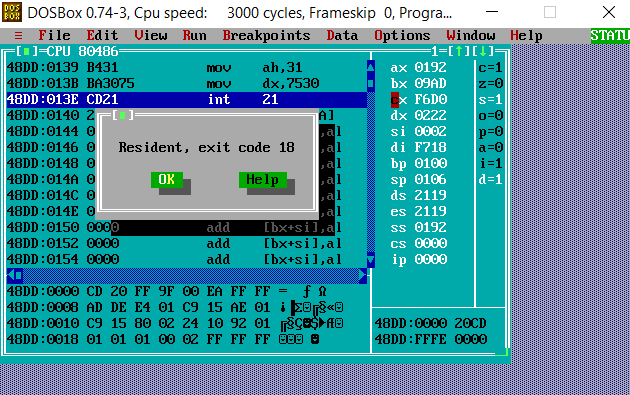


Однако в файле **DHOG68.ASM2** по-прежнему всё ещё ничего не записано:



Word-овский файл с отчётом также ещё не повреждён и спокойно открывается. То есть можно сделать вывод, что вирус повреждает файлы в **лексикографическом** порядке.

На всякий случай я довёл программу вируса до самого конца:



Так как мы подтвердили гипотезу, я посчитал, что не обязательно выводить имя самого первого (в лексикографическом, как мы выяснили, порядке) файла, который заражается вирусом.

Теперь приступим ко **2-ой части задания** – получению самой маленькой программы, которая делает что-то зримое для конечного пользователя.

Так как у меня нету ни времени, ни желания на разработку такой программы, я полез на помойку, чтобы поискать что-нибудь там…

Я подумал, что, наверное, самой маленькой и в то же время **делающей что-то зримое для пользователя** является та программа, котоаря выводит в терминал какое-то сообщение.

Я залез на вот этот ресурс [https://assembler-code.com/pervaja-programma-na-assemblere/](https://assembler-code.com/pervaja-programma-na-assemblere/%20) и нашёл там исходный текст некоторой программы, которая выводит в терминал «Hello, World!», поэтому для нашего случая я слегка изменил исходный текст так, чтобы программа выводила «Hello, User!!»:

.model tiny

.code

org 100h

start:

mov ah,9

mov dx,offset message

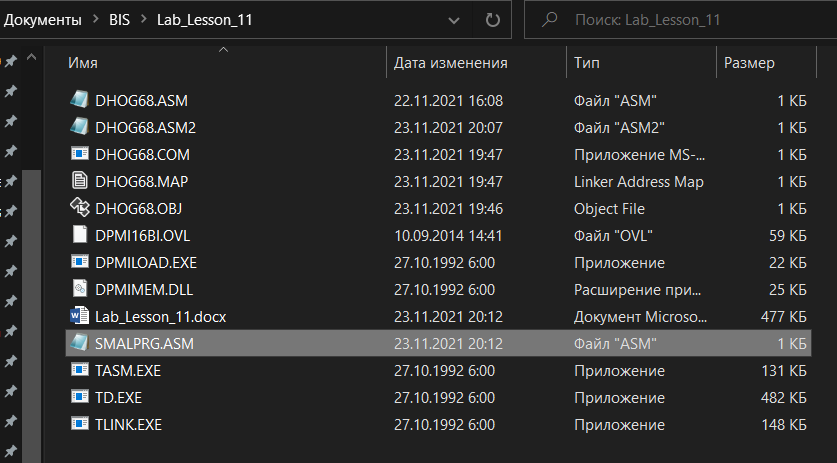
int 21h

ret

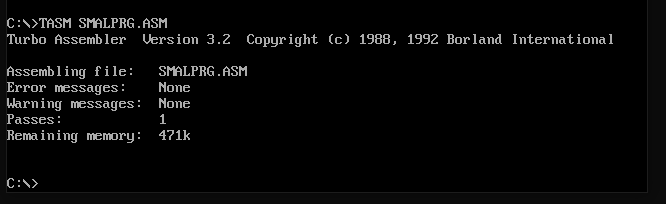
message db "Hello, User!!",0Dh,0Ah,'$'

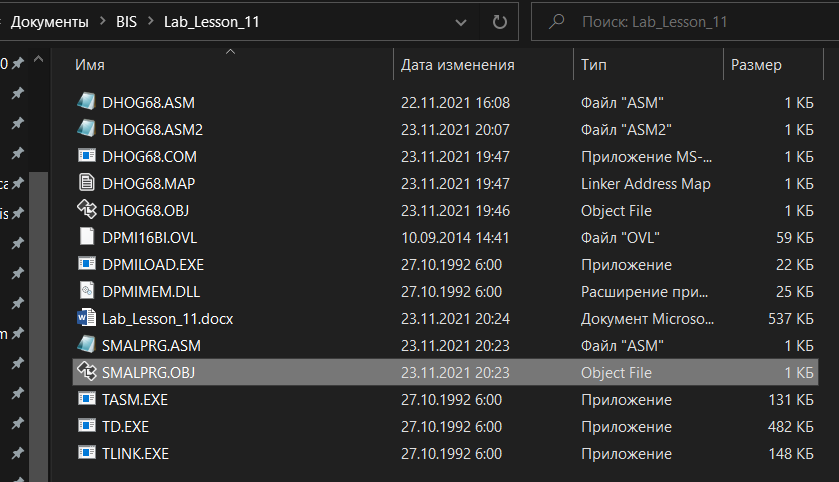
end start

Я сохранил данный исходный текст в файле **SMALPRG.ASM**:



Быстренько получим сначала объектный модуль **SMALPRG.OBJ**:



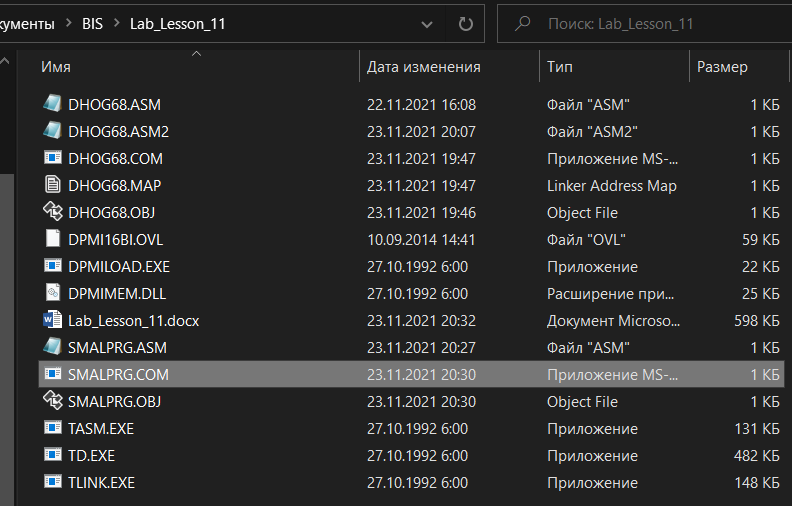


Затем получим исполнимый модуль **SMALPRG.СOM**:

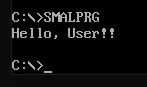


Для этого я прописал команду **TLINK /t /x SMALPRG.OBJ**. На помойке было указано собирать исполнимый модуль именно таким образом, потому я поробовал.

Исполнимый модуль появился:



После этого я запустил программу:



Таким образом мы получили одну из самых маленьких программ (можно было бы чуть-чуть меньше, если бы мы выводили не фразу, а один символ), после загрузки в оперативную память которой пользователь может **заметить** какие-то события в терминале.

На этом я закончил эксперименты.

В письме я постараюсь прикрепить архив, который будет включать в себя весь этот отчёт, исполнимые модули DHOG68.COM и SMALPRG.COM, исходные тексты DHOG68.ASM и SMALPRG.ASM, а также файл DHOG68.ASM2, внутри которого вирус успел записать свои машинные инструкуци.

Пароль от архива: **041** (на всякий случай, укажу пароль на самом верху этого отчёта тоже)