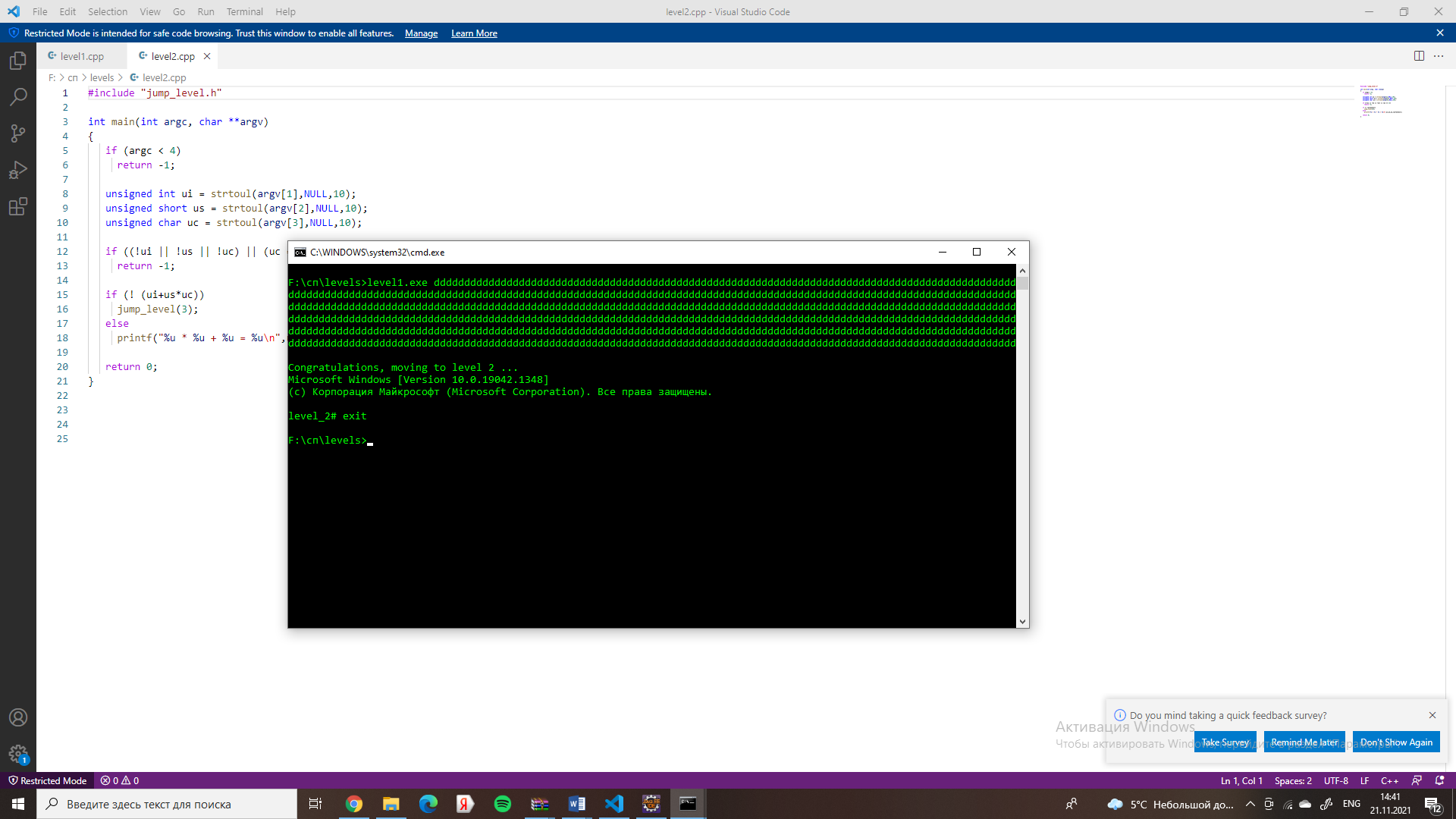
Отчет по Лабораторной работе 4

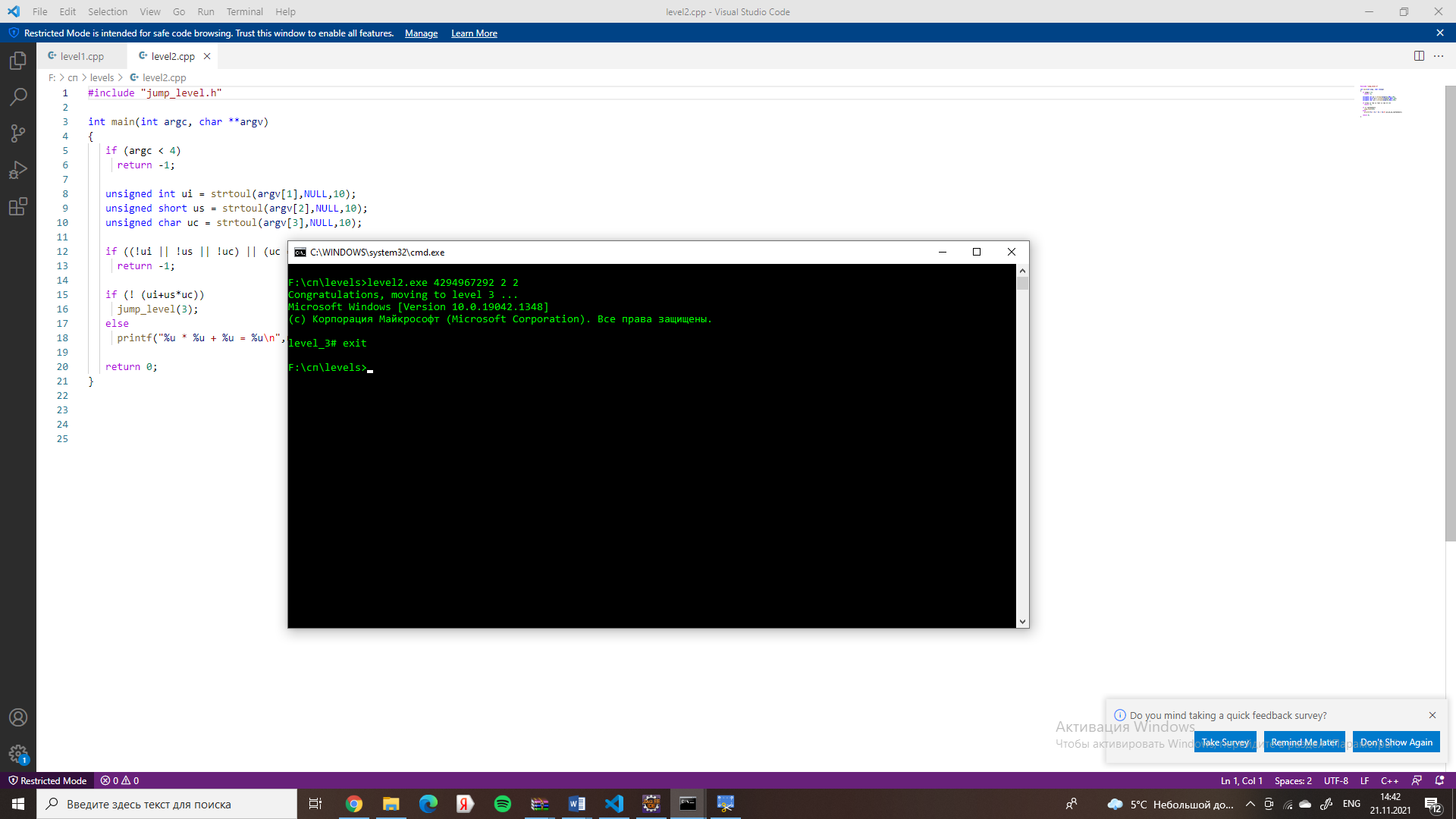
**Черненков Артём 13 группа**

№1



Передал строку, размер которой больше диапазона хранимых чисел char произошло переполнение – в первый бит попадет 1 c будет отрицательным.

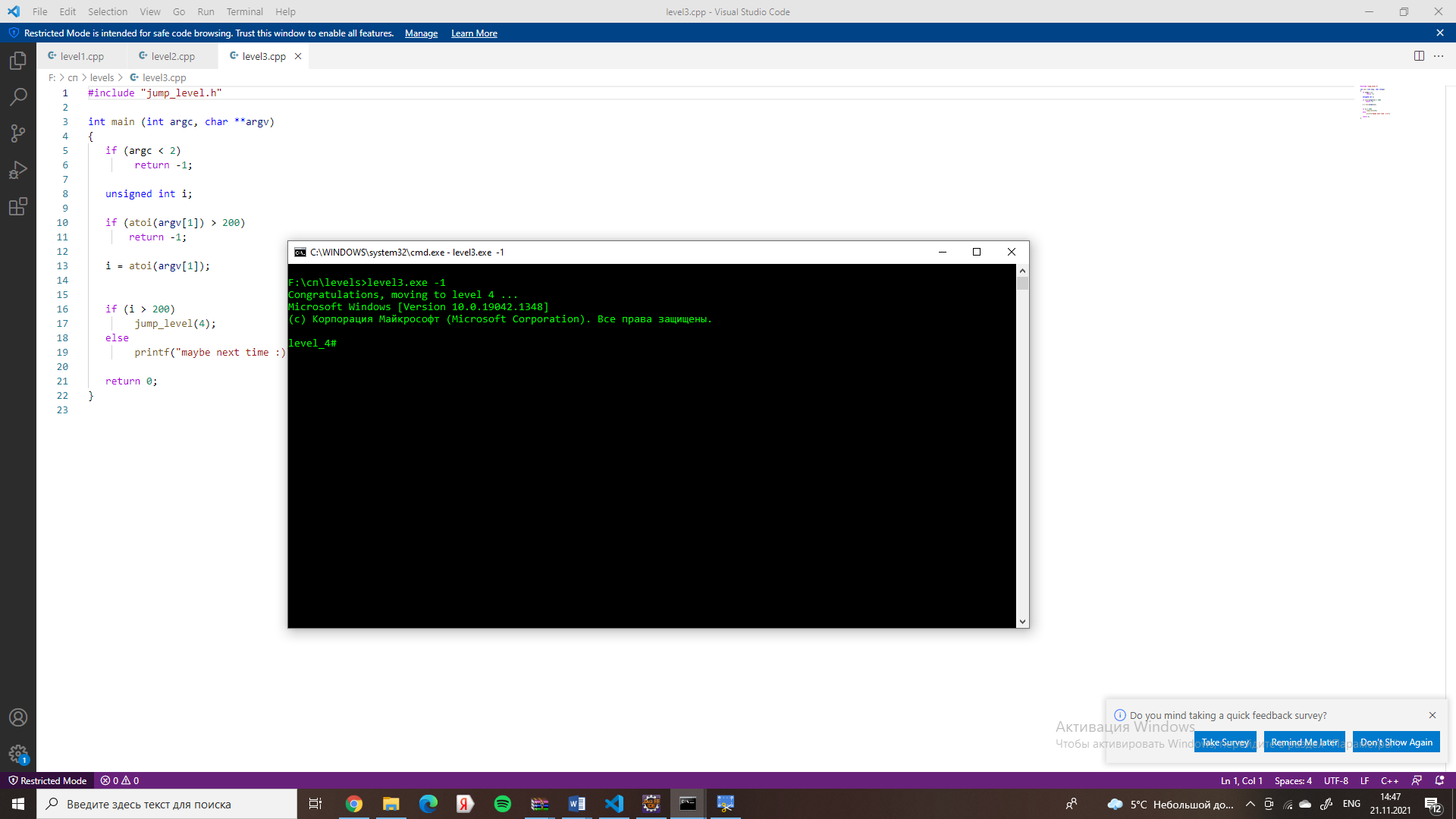
№2



Передаю 4294967292 2 2,

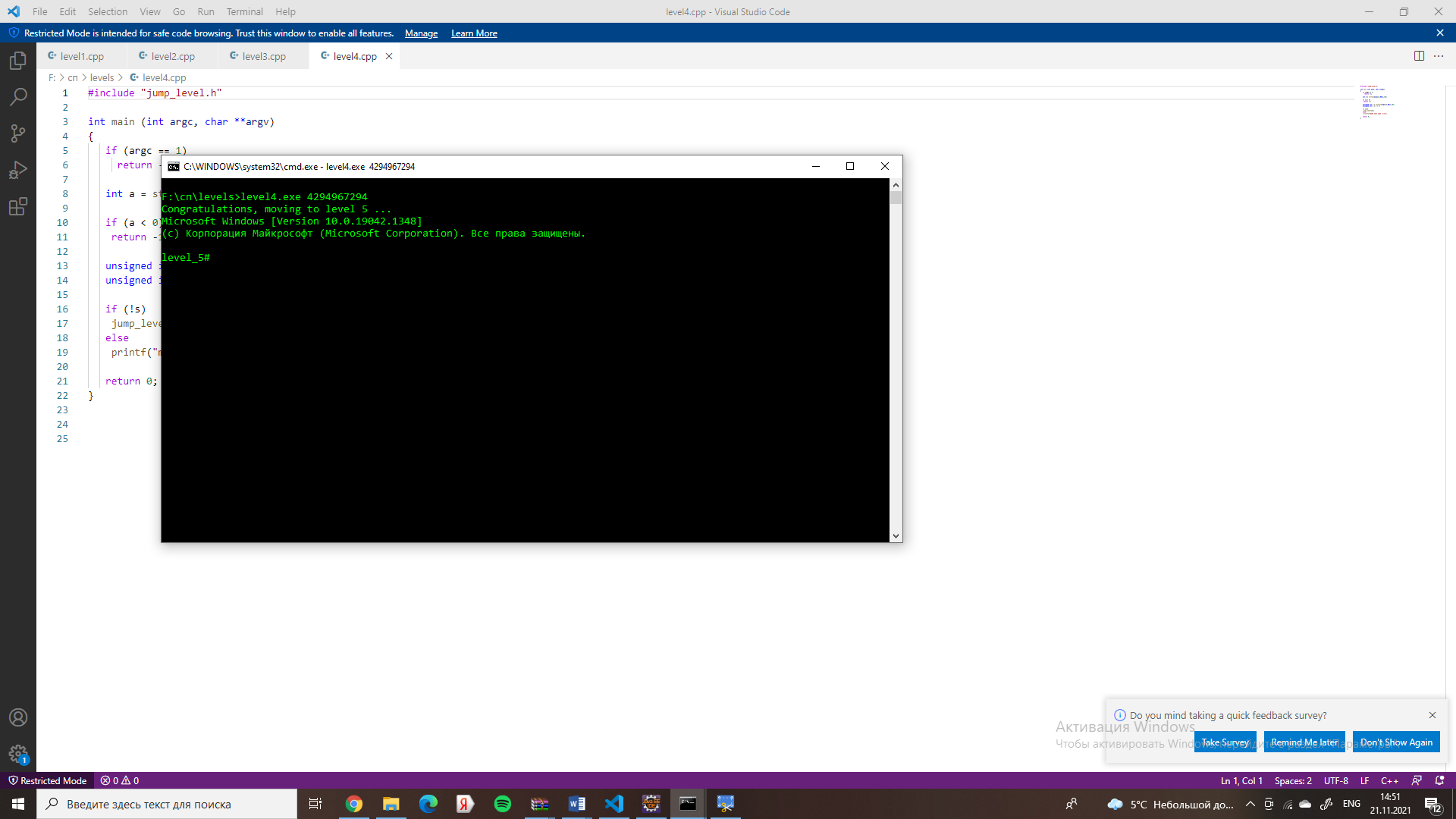
4294967295 – max unsigned int; (max unsigned int - 3) + 2 + 2 переполнение условие false.

№3



Передаём отрицательное число. При касте к unsigned знаковый бит будет интерпретироваться как часть числа полученное число > 200

№4

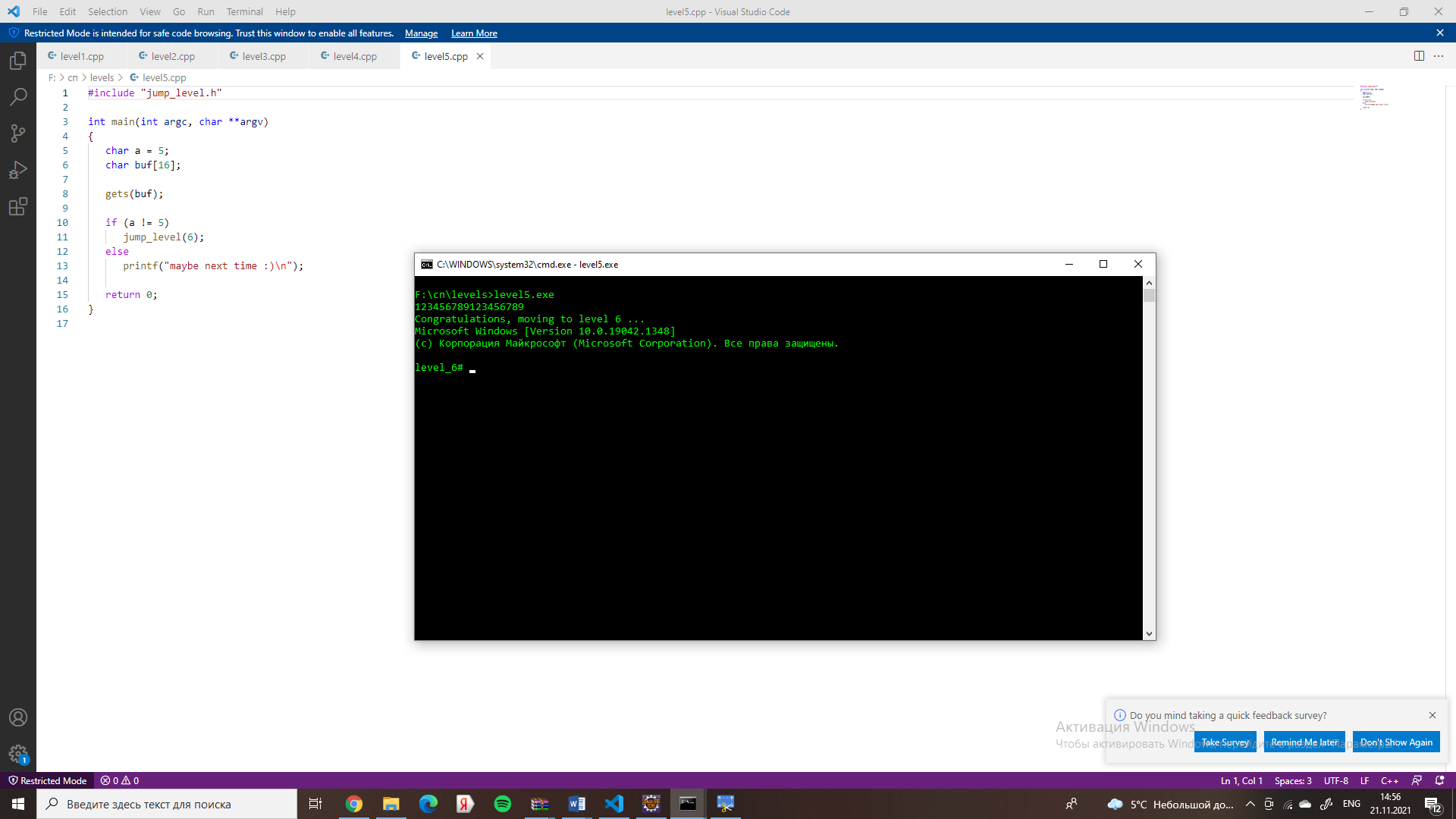


Max unsigned int = 4294967295

Чтобы получить 0 нужно передать (max unsigned int – 1), т.к. (max unsigned int – 1) + 2 = 0.

Передаю 4294967294

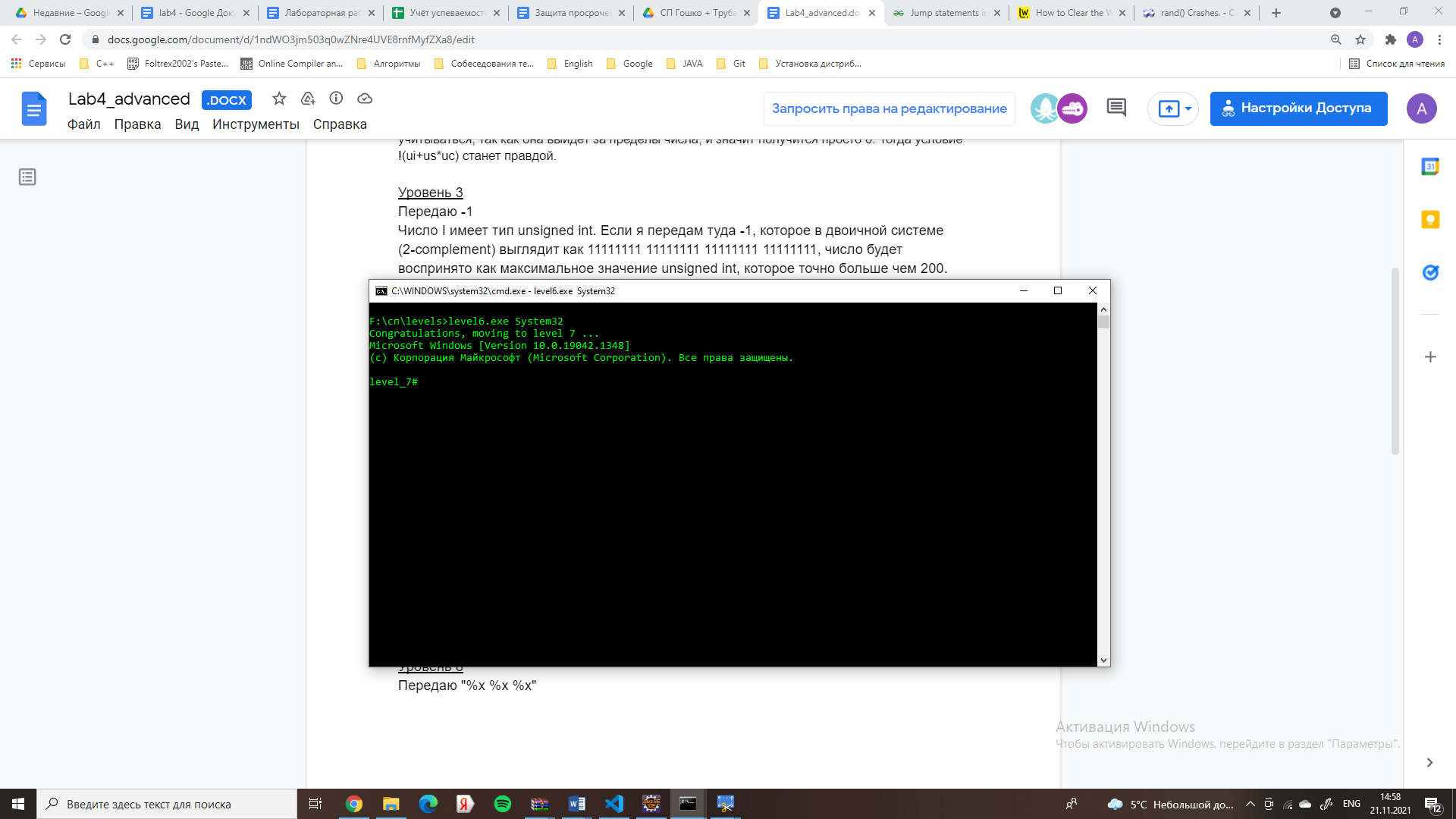
№5



Передаю > 15 символов

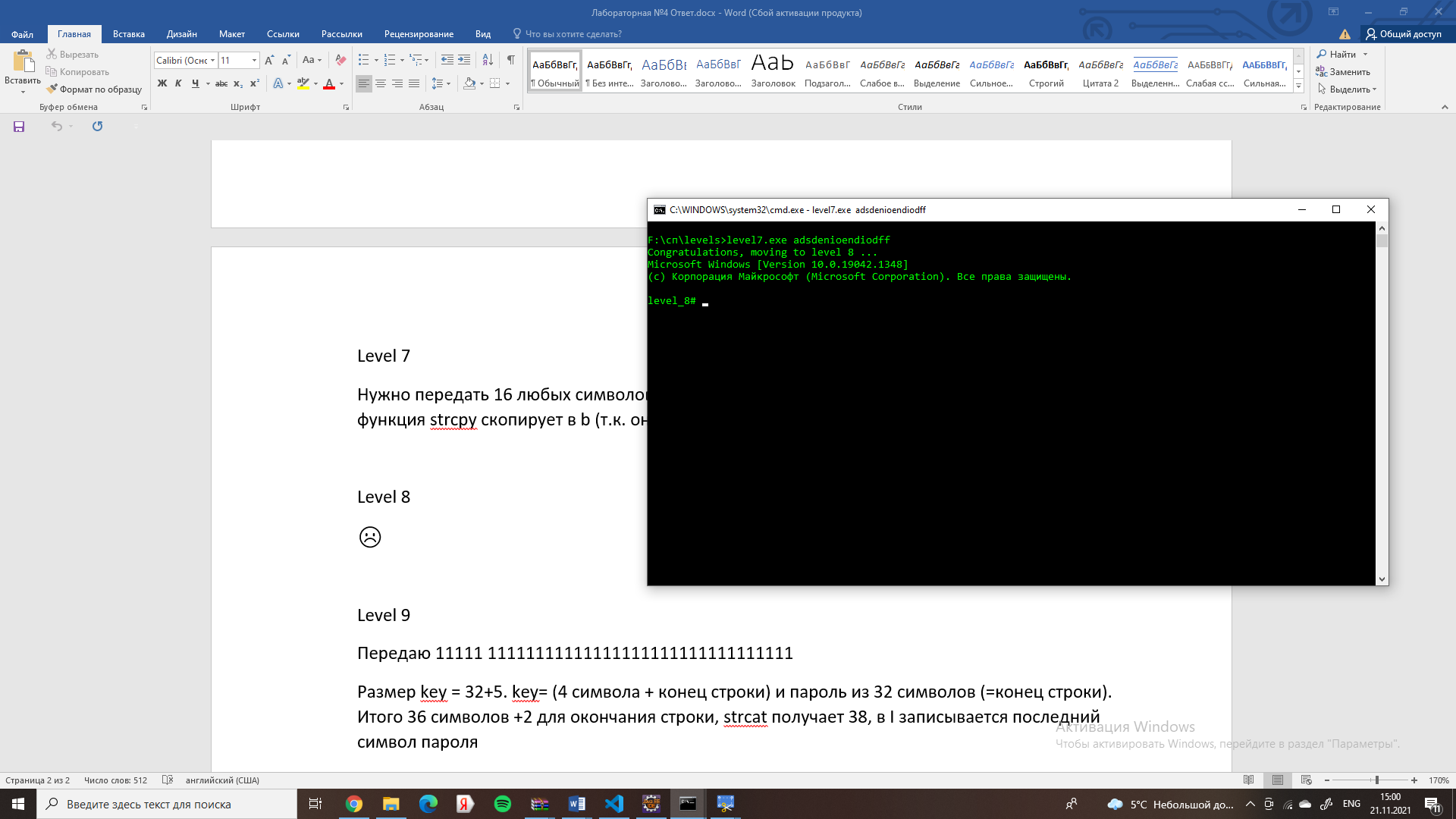
Т.к. на стеке переменная а хранится прямо под элементами массива, gets запишет значение buf[16] в переменную а.

№6



System32: папка с cmd.exe.

№7



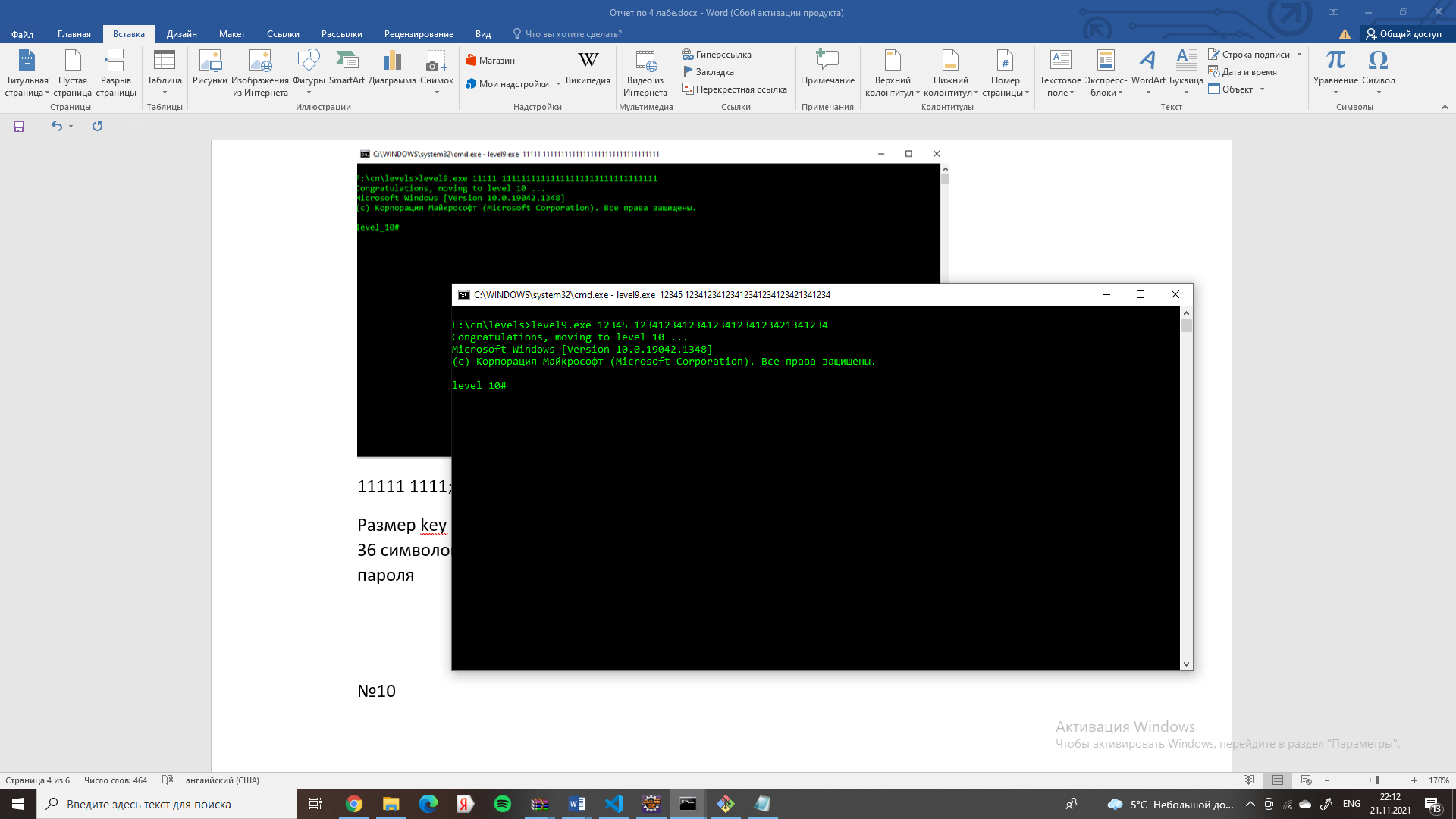
Передаю Ɐ16 символов. Тогда 17-й strcpy скопирует в b: она выше в стеке. Если передать больше, то изменится b.

№8

"%x %x %x"

Printf получает такую строку-формат, подставляет в нее три следующих своих аргумента (точнее их hex) и выводит. Аргументы он ищет на стеке, но, т.к. ему ничего не передали, там будут адрес возврата и адрес строки формата, а третьей по счету будет идти искомая переменная I.

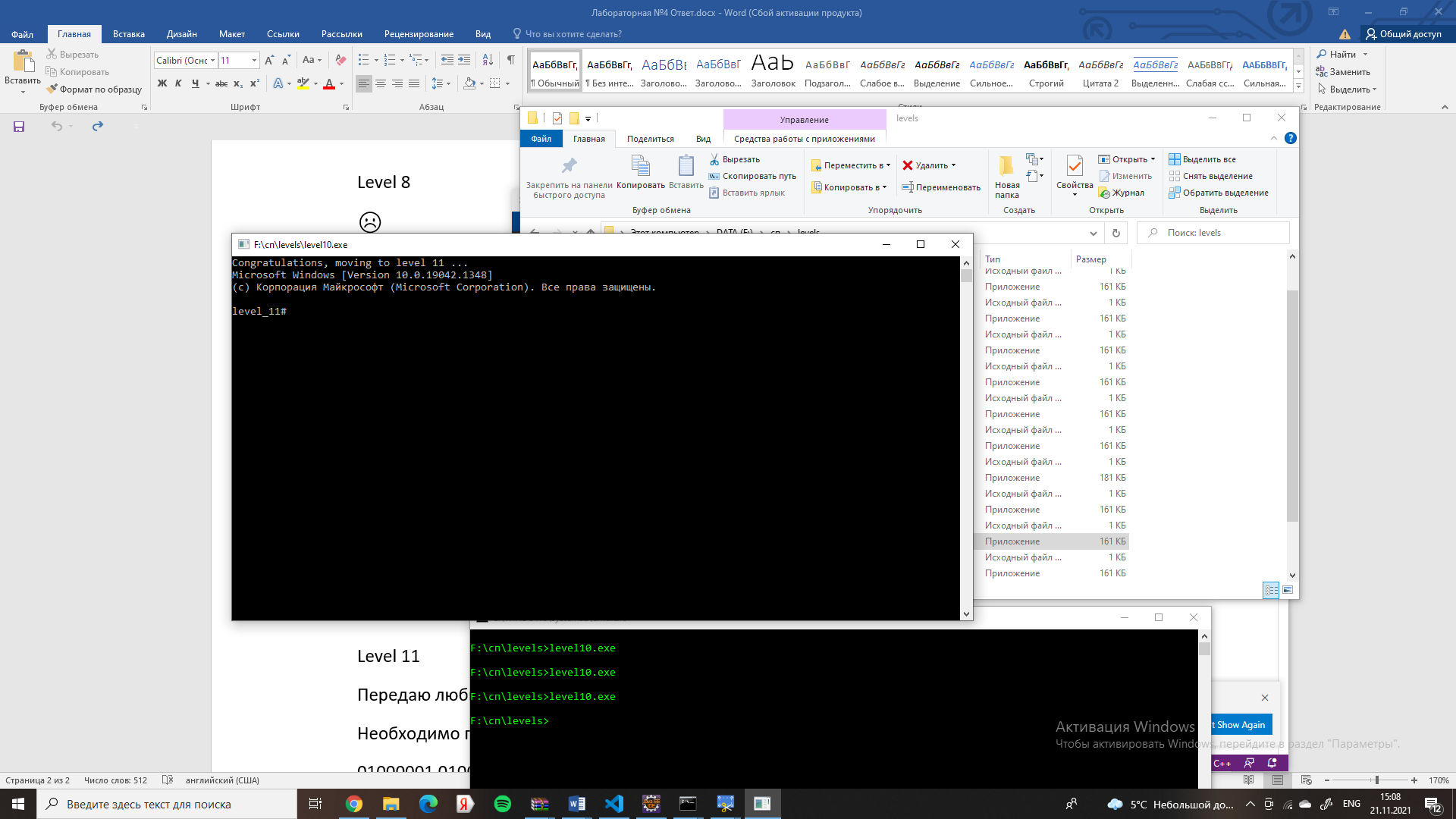
№9



12345 1234'1234’1234’1234’1234’1234’1234’1234

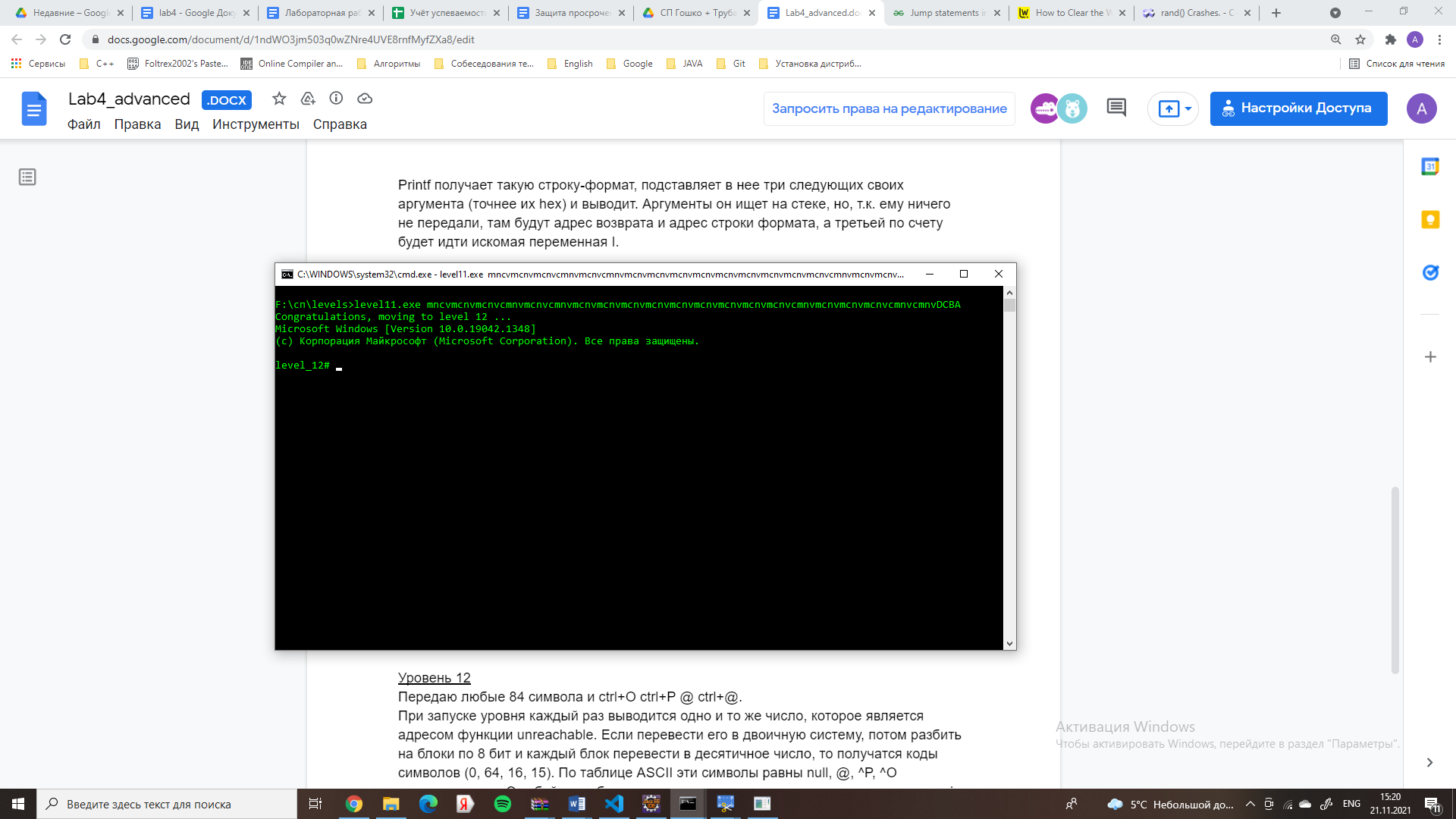
Key size = 37. Key = 4 characters+ ‘\0’ + 32 characters + ‘\0’. strcat получает 38, в i записывается последний символ пароля

№10



Запускаю level10.exe, ничего не передавая. argv[0] - путь к исполняемому файлу( > 16 characters). После цикла I = 16 0 запишется в buf[16], который представляет собой I, т.к. в стеке переменные размещаются в системном стеке, где адреса идут в обратном порядке, т.е. адресI > адрес массива

№11



Ɐ84 символа + DCBA.

Необходимо получить в eip 0x41424344. Это число равно

0b01000001 01000010 01000011 01000100. На стеке saved\_eip, saved\_ebp (4 байта) и buf (80 байт). Если передать строчку из 88 байт, то первые 80 скопируются в buf, следующие 4 байта в saved\_ebp, а последние 4 байта в saved\_eip.

Если перевести каждый блок бинарного числа в символы, то получится ABCD. Но так как в стеке число лежит от младшего байта к старшему, то нужно вводить в обратном порядке

№12

Ɐ84 символа + (char)15 + (char)16 + (char)64 + (char)0

Можно либо через каретную нотацию, либо скопировать в консоль эти символы.

При запуске уровня каждый раз выводится одно и то же число, которое является адресом функции unreachable. Если перевести его в двоичную систему, потом разбить на блоки по 8 бит и каждый блок перевести в десятичное число, то получатся коды символов (0, 64, 16, 15). Эти символы в обратном порядке нужно записать в адрес возврата main, чтобы после выхода из неё запустилась функция unreachable.