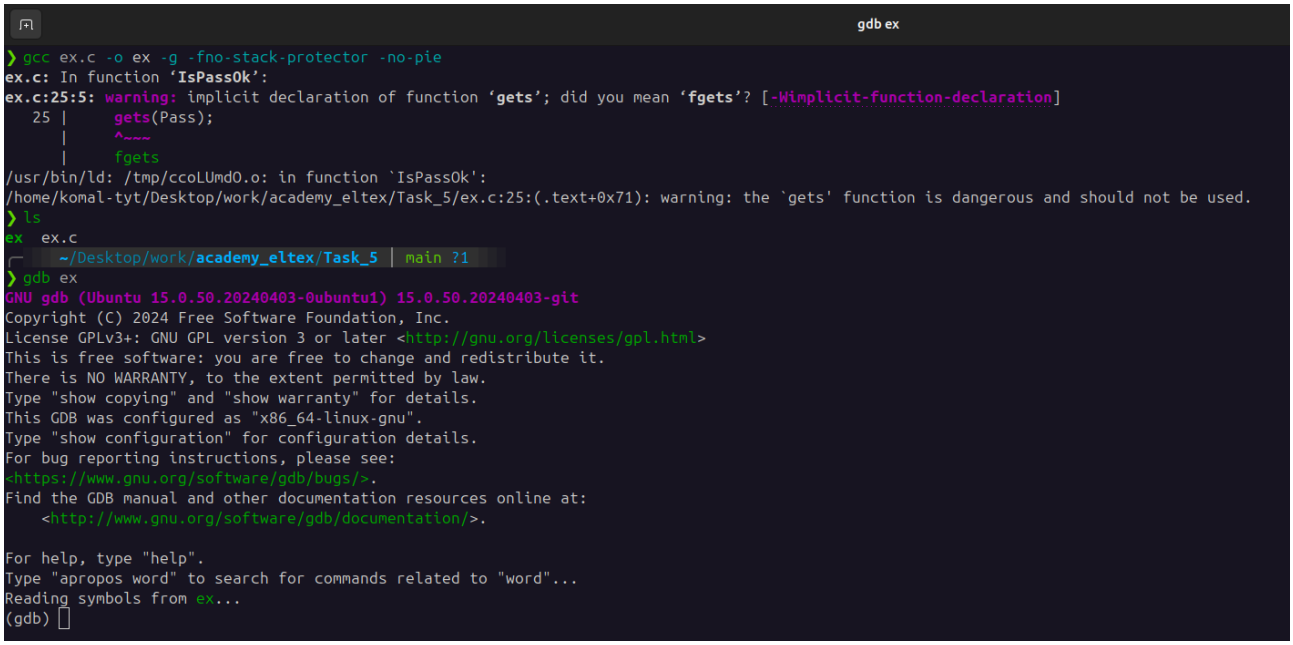
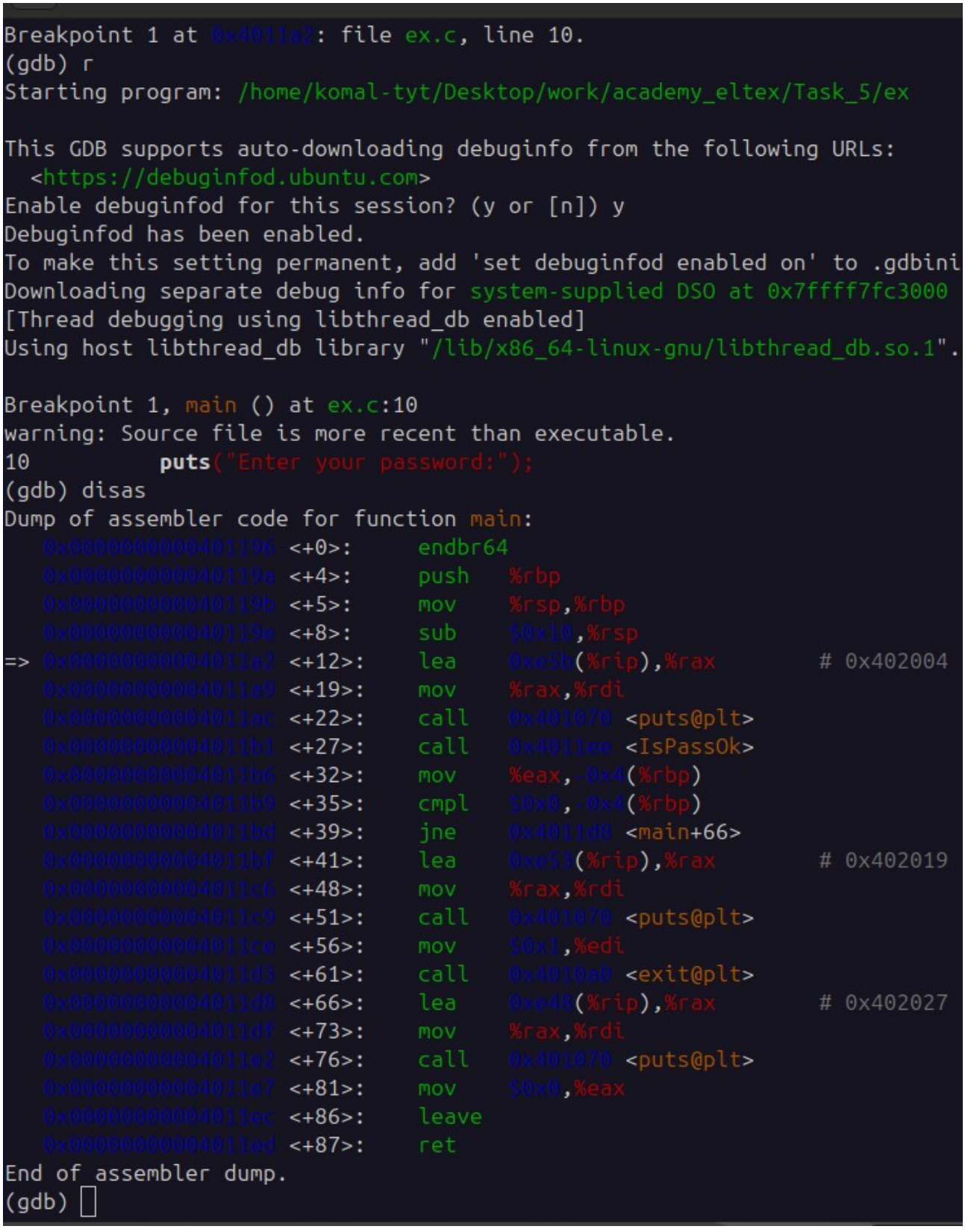
ОТЧЕТ

Домашнее задание №5 — Функции

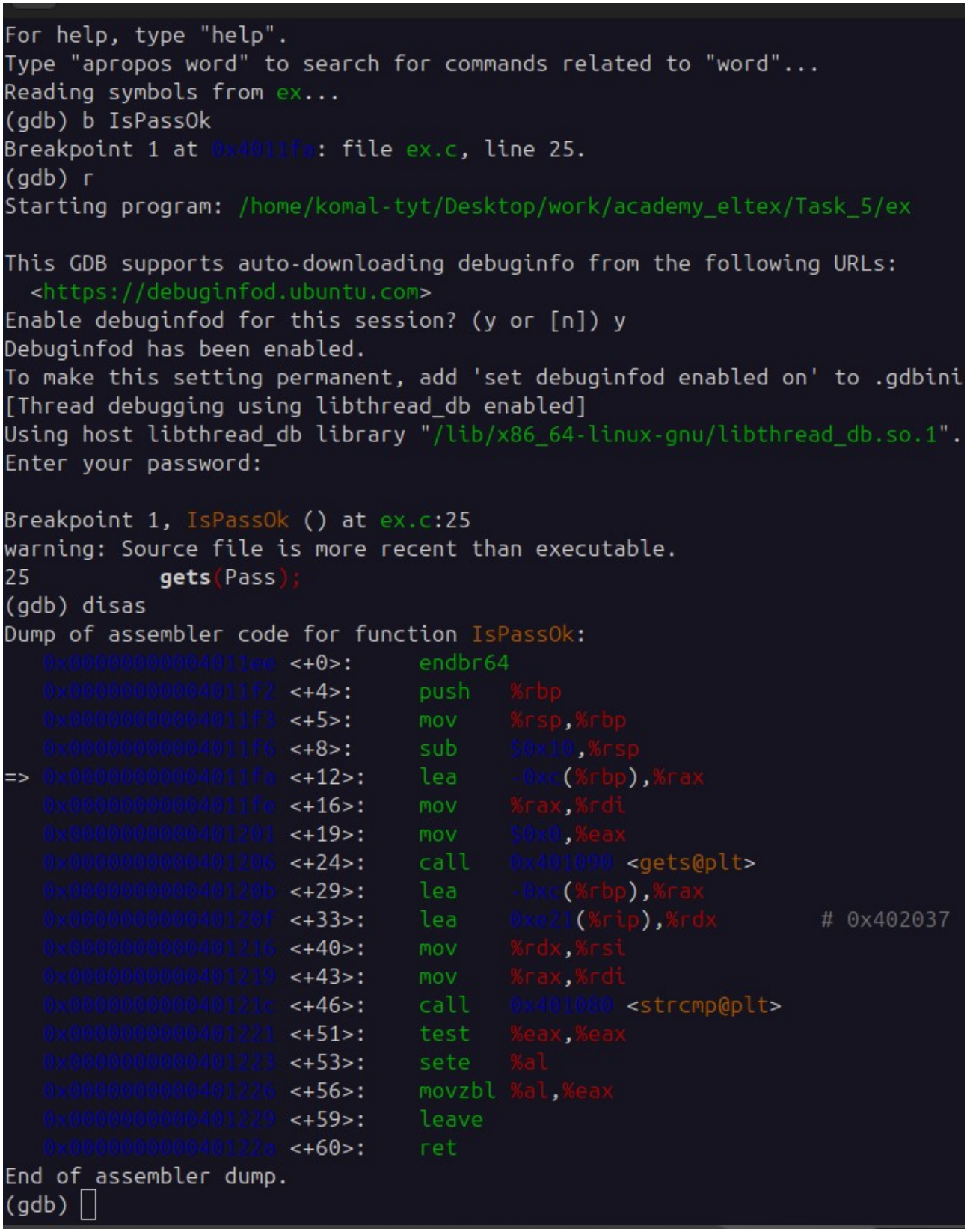
Выполнил: Коваленко Дмитрий



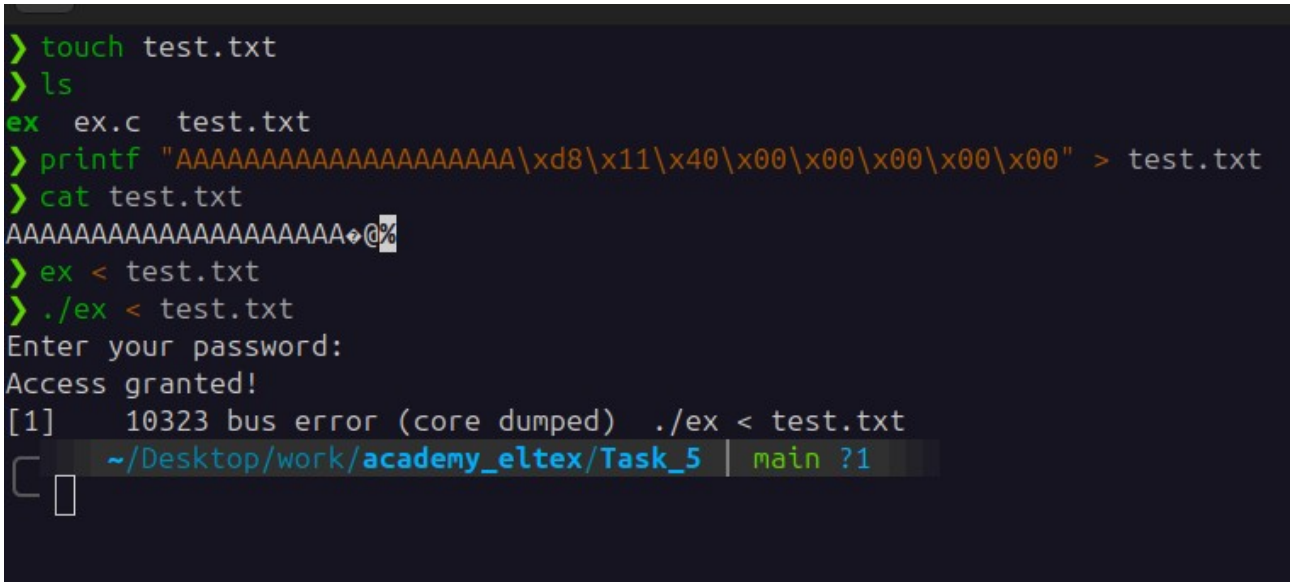
1) Первым делом скомпилировал программу с нужными параметрами и запустил отладчик gdb



2) Поставил breakpoint на функцию main, дисассемблировал и нашел адрес возврата ветки, где пароль подошел корректно это 0x00000000004011d8



3) Потом тоже самое сделал с функцией IsPassOk. Надо посчитать через сколько байт начинается адрес возврата на функцию main, как я понял на адресе 0x00000000004011fa выделяется 12 байт на массив Pass, далее идет 8 байт на сохраненный rbp и следующие 8 байт на адрес возврата, то есть 12 + 8 = 20 байт, а после идет как раз таки 8 байт адреса возврата, который нам нужно перезаписать.



4) Создал txt файл, чтобы записать в него 20 байт каких-то символов, а дальше 8 байт адреса возврата на нужную нам ветку в функции main.