НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Практична робота № 4

з дисципліни

“Основи захисту інформації”

Варіант 4

Виконала:

студентка групи ІС-71

Вознюк О. В.

Перевірив:

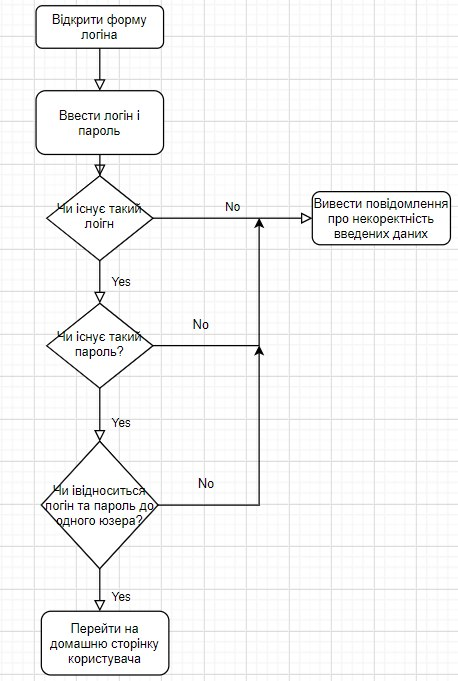
аспірант

Ільїн К. І.

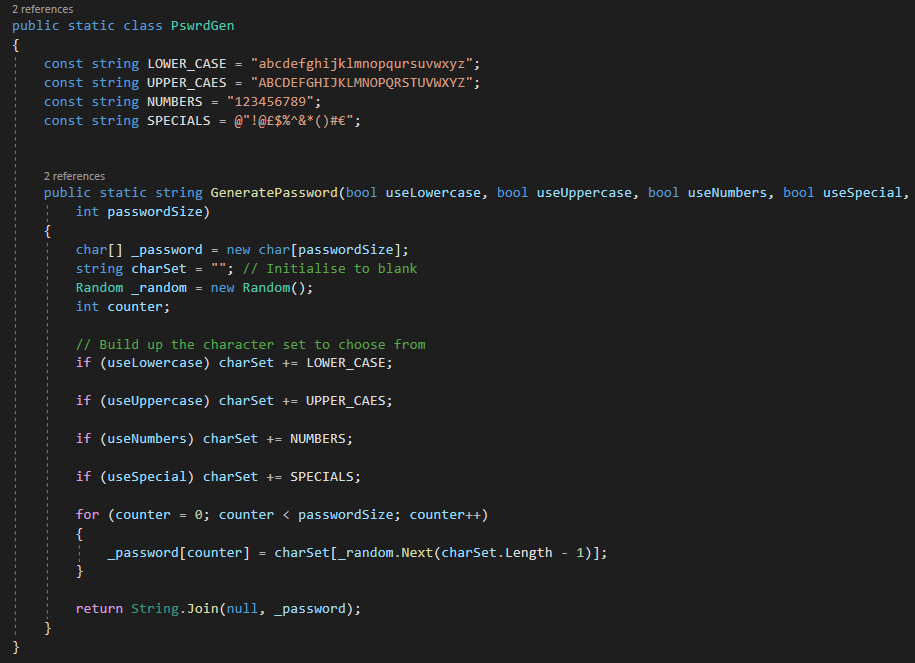
Київ-2020

**Хід виконання роботи**

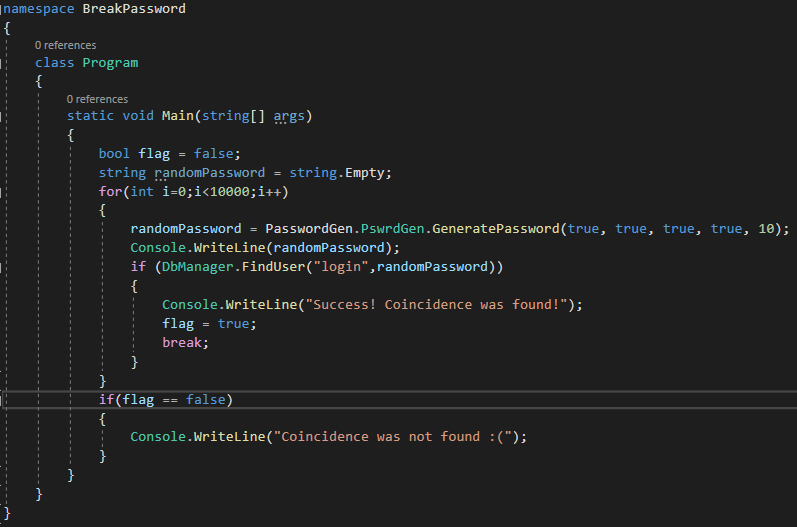
1. Була створена програма для аналізу.

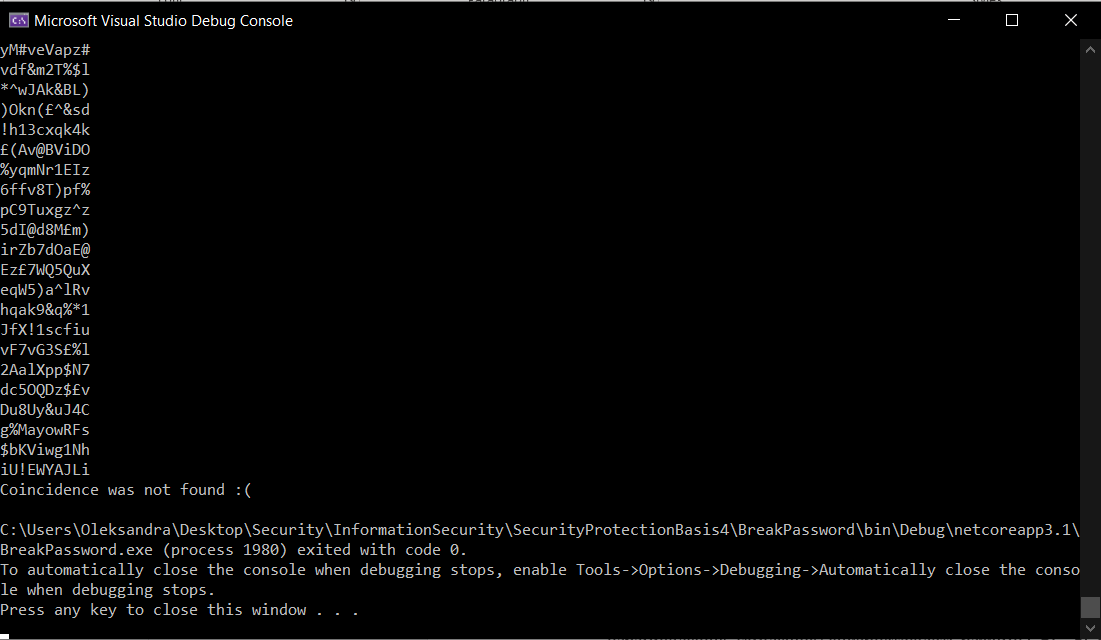


1. Був створений клас для генерації паролів.

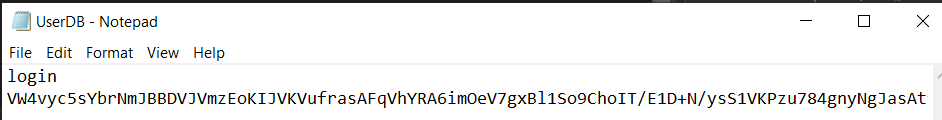


1. Була створена програма для підбору паролю для юзера для якого відомий логін.

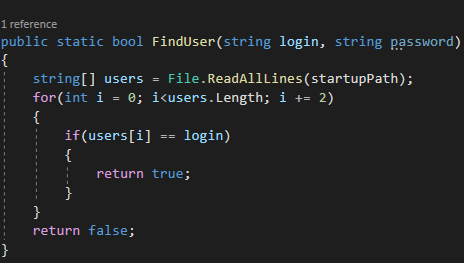




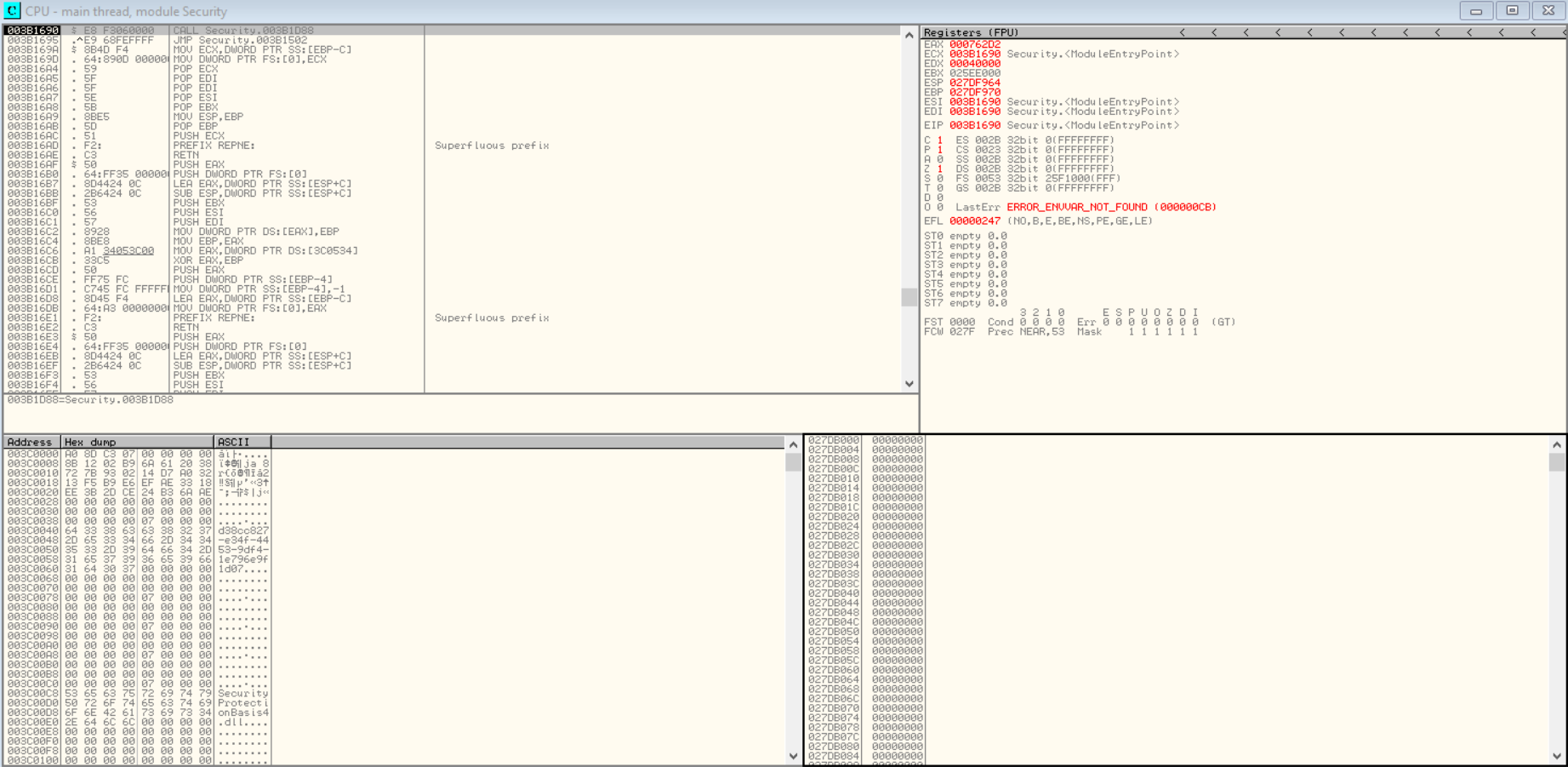
1. Вигляд бд, де зберігаються записи зареєстрованих юзерів (логін та пароль, де пароль у зашифрованому вигляді).



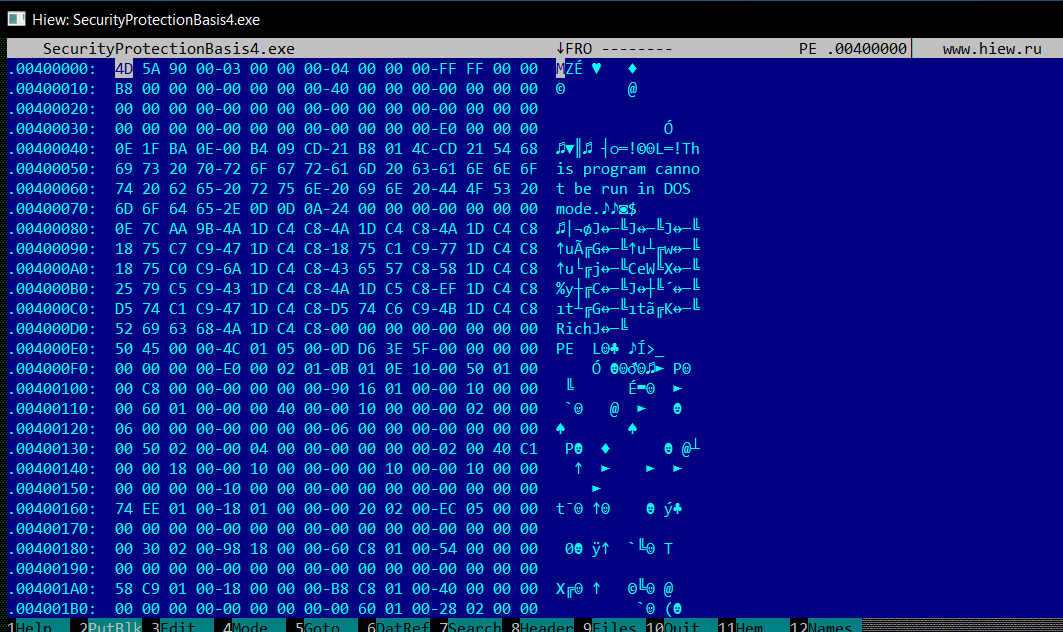
1. Модіфікована функція (прибрано порівняння введеного пароля із записаним у зашифрованому вигляді в бд, таким чином можна здійснити вхід тільки за допомогою правильно введеного логіну)



1. Аналіз програми, що аналізується в OllyDBG



1. Аналіз програми, що аналізується в Hiew.



**Відповіді на теоретичні питання**

1. Які методи та прийоми використовуються для захисту додатку від дослідження?  
Універсальним методом протидії дизасемблерування програми є шифрування. Підсилює захист динамічне шифрування і багатопрохідна розшифровка коду.  
(Дизасе́мблер — комп'ютерна програма що транслює мову машинних кодів у мову асемблер.)  
Для захисту від статичного вивчення алгоритму отримання і перевірки ключової інформації в середовищі запуску захист програми відбувається за допомогою дисасемблера і декомпілятора зазвичай застосовується самомодифікуючий код, що вимагає використання при розробці системи захисту мови асемблера. Якщо це неможливо, то застосовуються методи «заплутування» програмування (так зване обфускація), спрямовані на максимальне ускладнення розуміння алгоритму роботи системи захисту шляхом максимального «заплутування» її коду.  
Для ускладнення розуміння алгоритму перетворення отриманої ключової інформації при її перевірці можуть застосовуватися такі методи:  
• використання асиметрично шифрування:  
1) користувач повідомляє правовласнику персональні дані;  
2) правовласник шифрує їх за допомогою свого секретного ключа і повертає користувачеві разом з програмою і своїм відкритим ключем;  
3) при запуску програми система захисту розшифровує за допомогою отриманого відкритого ключа дані користувача і порівнює їх з введеними їм даними;  
• використання при перевірці ключової інформації функції хешування;  
• використання нейронної мережі зворотного поширення, навченої на апроксимацію функції перетворення ключових даних;  
  
2. Чому зворотне дослідження застосунку, написаного на мові Java чи С# (.NET) здійснюється легше, ніж для того, що написаний на мові С?  
В Java та С# (.NET) є рефлексія коду, на мові С це зробити практично неможливо.  
3. Які засоби використовують віруси для протидії їхньому дослідженню?  
Антивірусна - спеціалізована програма для виявлення комп'ютерних вірусів, а також небажаних (що вважаються шкідливими) програм, відновлення заражених (модифікованих) такими програмами файлів і профілактики - запобігання зараженню (модифікації) файлів або операційної системи шкідливим кодом.  
4. Які характеристики шкідливого ПЗ, одержані в ході зворотного дослідження, можна використовувати для його класифікації та кластеризації?  
Поведінкові ознаки

**Висновок**

Було досліджено принцип роботи у програмах Hiew та OllyDbg. Були отримані навички модифікації бінарного коду застосунку та взлому захисту програми.