НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Практична робота № 1

з дисципліни

“Основи захисту інформації”

Варіант 4

Виконала:

студентка групи ІС-71

Вознюк О. В.

Перевірив:

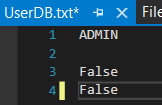
аспірант

Ільїн К. І.

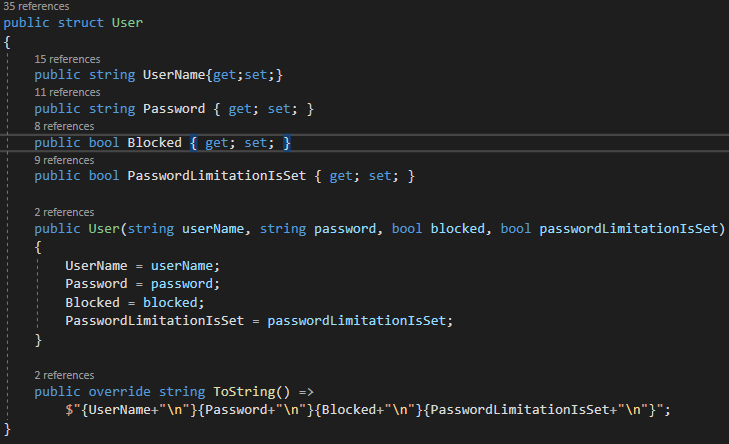
Київ-2020

**Хід виконання роботи**

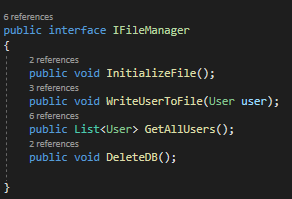
1. Було вирішено зберігати дані про користувачів у txt файлі, де кожне поле зберігається з нового рядка у порядку: ім’я користувача, пароль користувача, чи юзер заблокований, чи має юзер обмеження на встановлені паролі. При першому запуску програми файл містить тільки запис про адміністратора.

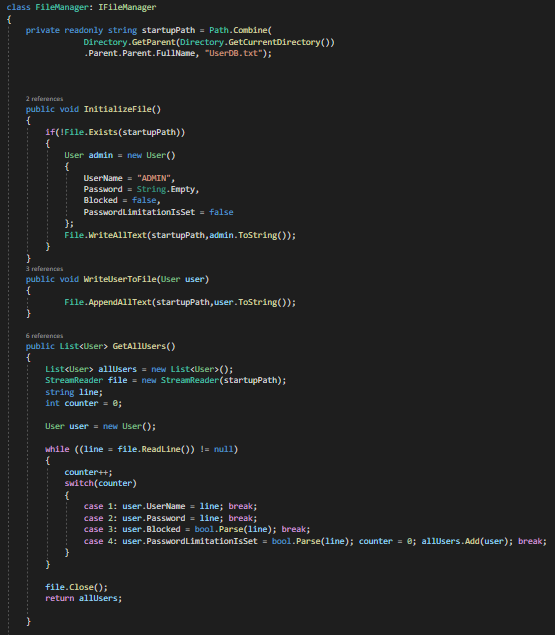


1. Далі була створена структура для представлення користувача (як звичайного так і адміністратора)

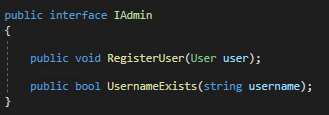
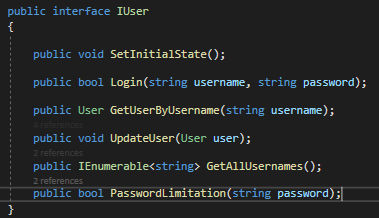


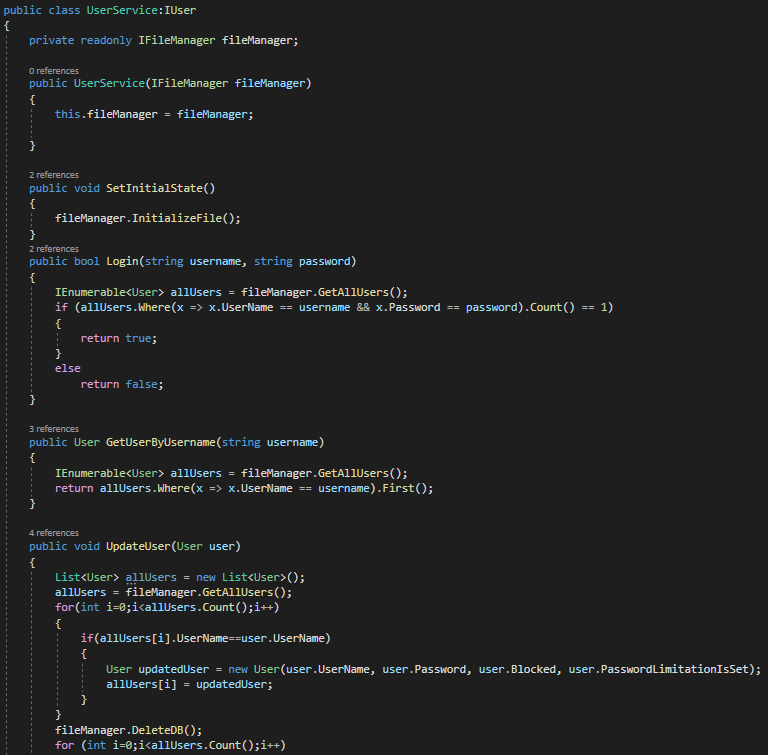
1. Був створений клас для доступу до бази даних (файлу txt) і його інтерфейс

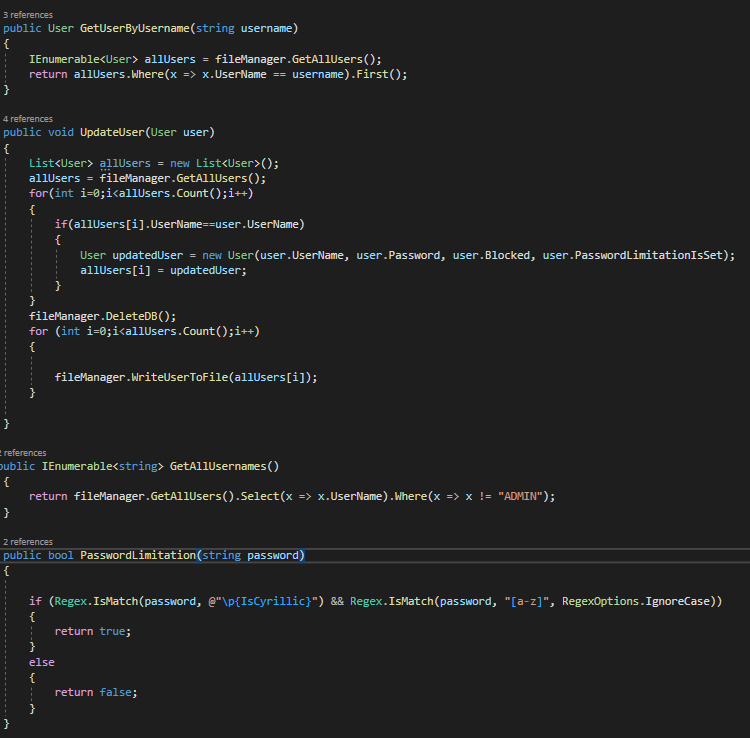


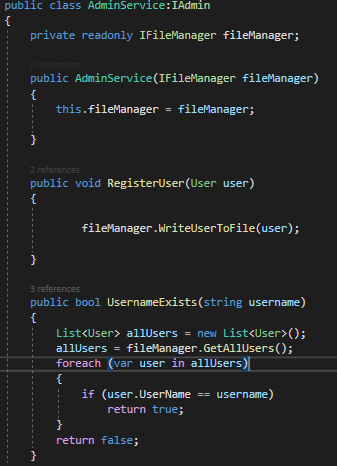


1. Були створені сервіси UserService та AdminService та їх інтерфейси для взаємодії з классами форм.

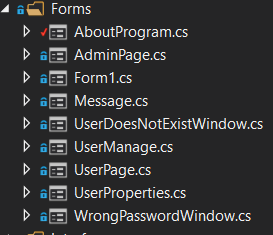




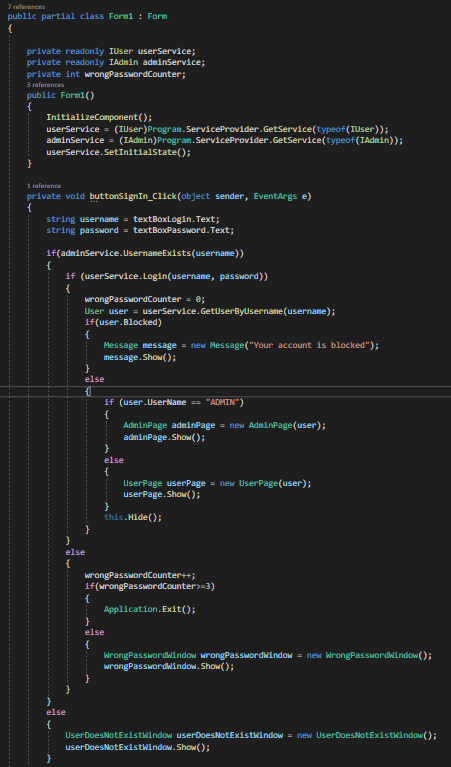


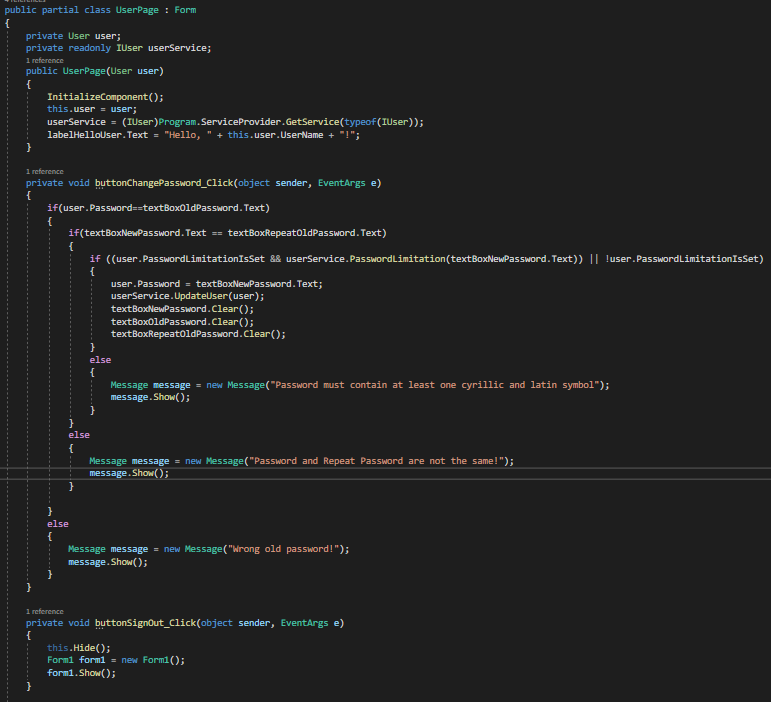


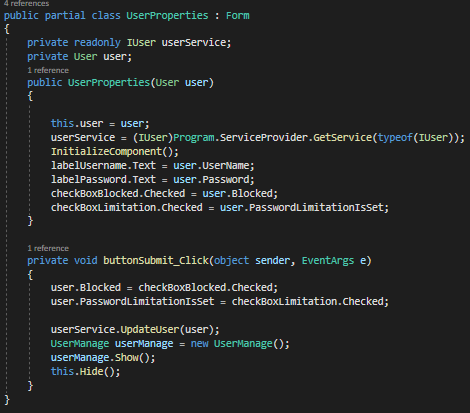
1. Наостанок були створені форми, що є інтерфейсом для користувачів.

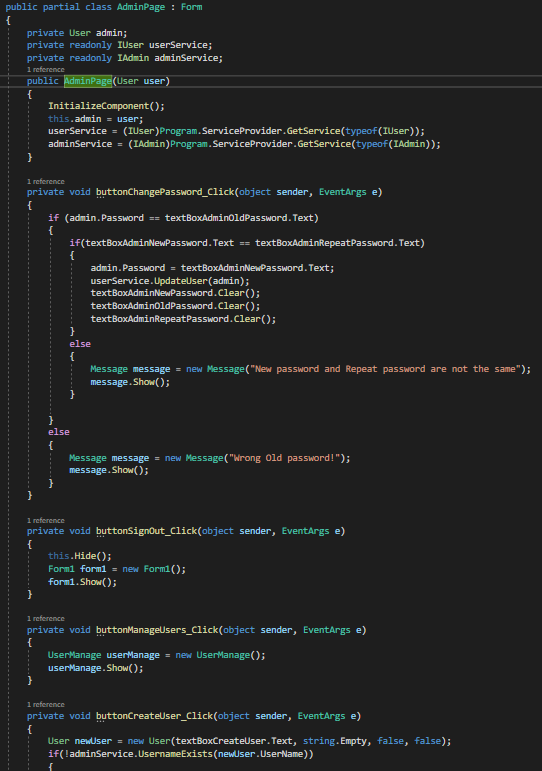


1. Нижче приведена логіка основних форм програми.

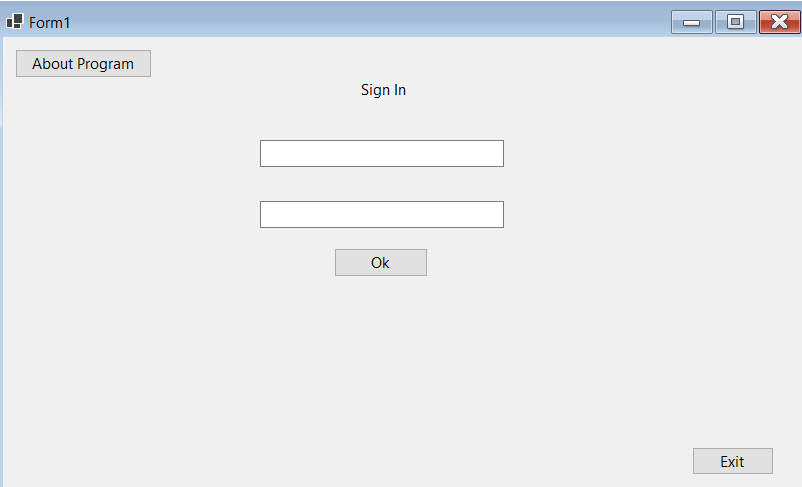


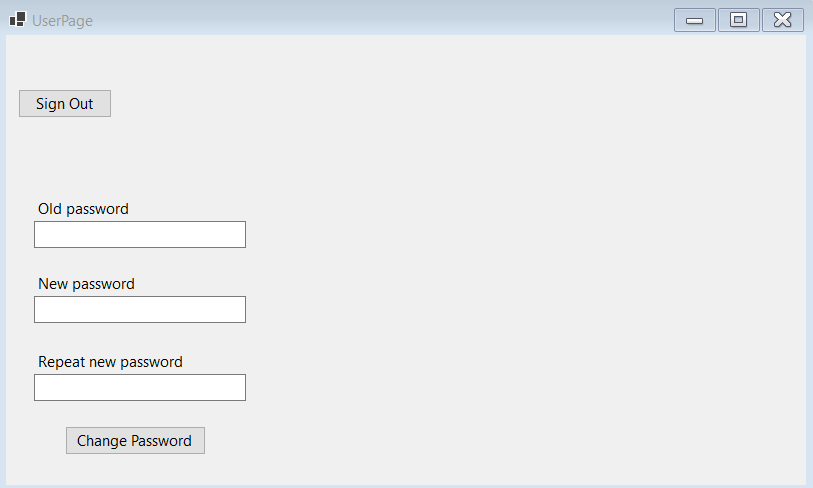
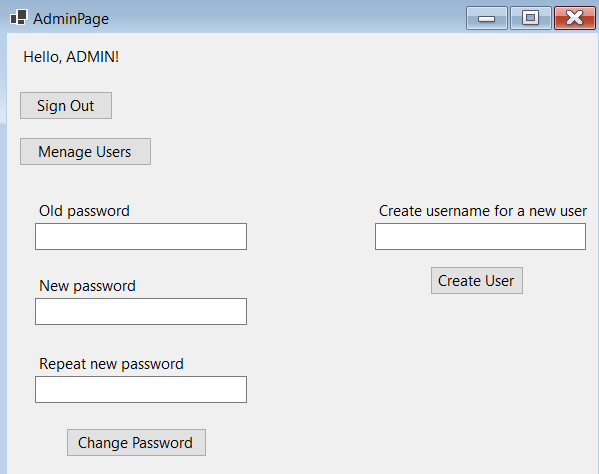


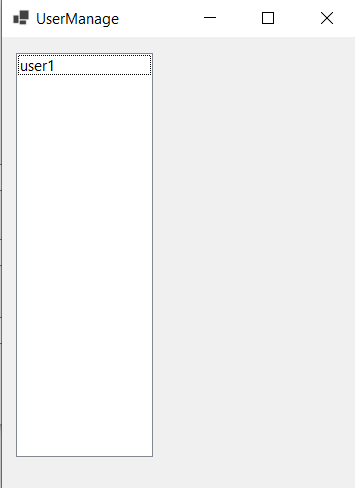
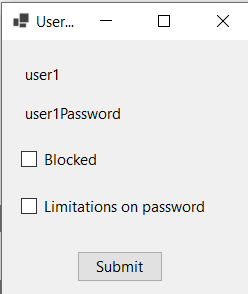




1. Нижче приведений зовнішній вигляд основних форм програми.







**Відповіді на теоретичні питання**

1) Які засоби захисту паролів при їх зберіганні використовує операційна

система.

* Накладення технічних обмежень;
* Керування терміном дії пароля;
* Обмеження доступу до файлу пароля;
* Обмеження числа невдалих спроб;
* Використання програмних генераторів паролів;

2) Види автентифікації: проста парольна, біометрична, автентифікація на

основі списку паролів. Відмінності та недоліки.

* Парольна – за допомогою встановлення паролю. Недоліки – часто паролі роблять очевидними, які не важко вгадати, або не зберігають у секреті їх.
* Біометричнв – за допомогою аналізу унікальних характеристик людини. Недоліки – біометричні методи дорогі і складні в обслуговуванні, низька достовірність, призначені тільки для аутентифікації людей.
* На основі списку паролів – за допомогою встановлення списку паролей. Більш надійний спосіб ніж проста парольна автентифікація.

3) Сaptcha та ReCaptcha – які недоліки системи веб-автентифікації вони

ліквідують,

Captcha дозволяє визначити чи є людина комп’ютером чи ні за допомогою спеціального теста згенерованого комп’ютером. Recaptcha є типом Captcha.

4) Двофакторна автентифікація. Сфера застосування, приклади.

Забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів. Прикладом є авторизація Google та Microsoft, де крім введення логіну та паролю потрібно ввести згенерований код, що приходить користувачеві у вигляді смс, електронного листа і тд. Також такий тип автентифікації застосовується в онлайн-банкінгах.

**Висновок**

Був реалізований алгоритм розмежування користувачів на основі парольної автентефікації. Були визначені такі переваги використання парольної автентифікації як простота та зручність для користувача і такі недоліки як порівняно слабкий захист особливо при слабкому паролі та необізнанності користувача як правильно зберігати паролі. Також був реалізований парольний захист у вигляді накладення технічних обмежень та обмеження числа невдалих спроб при введенні пароля.