НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”

КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Практична робота № 2

з дисципліни

“Основи захисту інформації”

Варіант 4

Виконала:

студентка групи ІС-71

Вознюк О. В.

Перевірив:

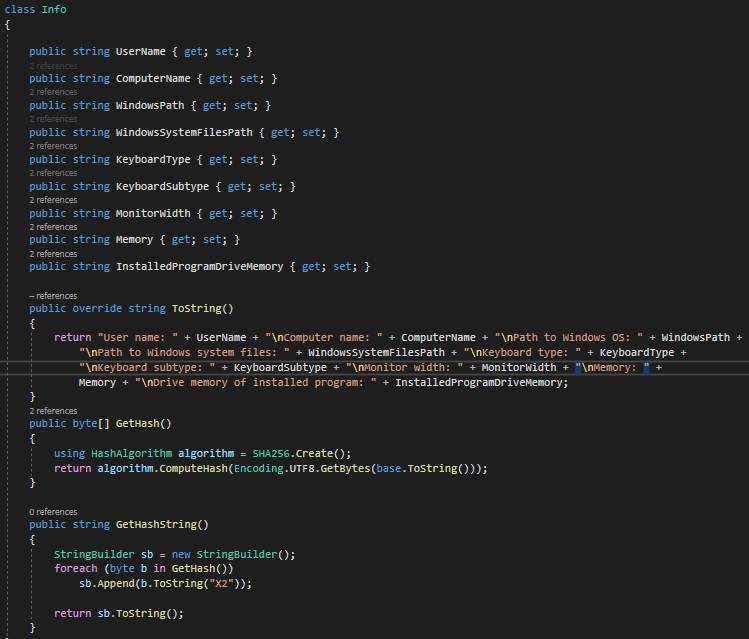
аспірант

Ільїн К. І.

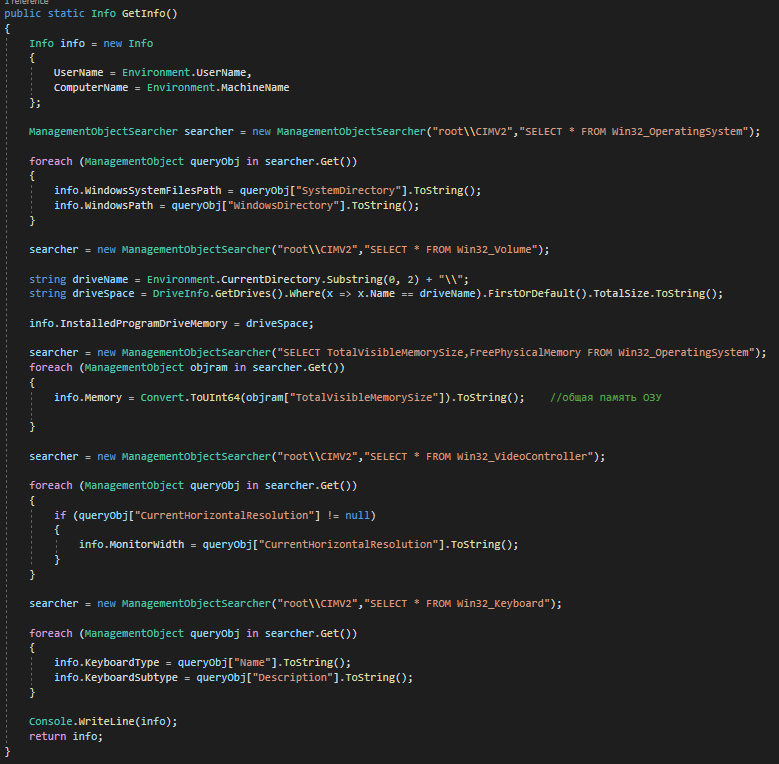
Київ-2020

**Хід виконання роботи**

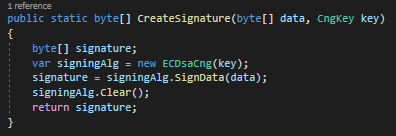
1. Був створений клас для збереження даних, а також її хешування

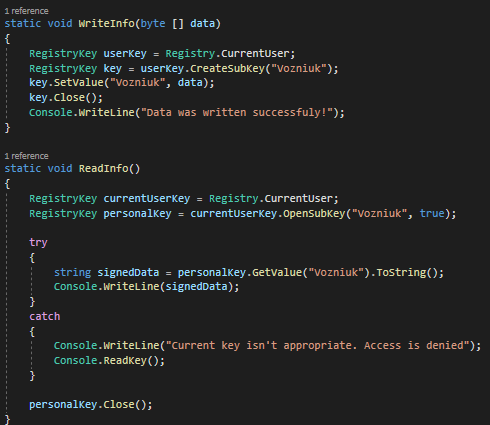


1. Був створений метод для отримання інформації з комп’ютера.

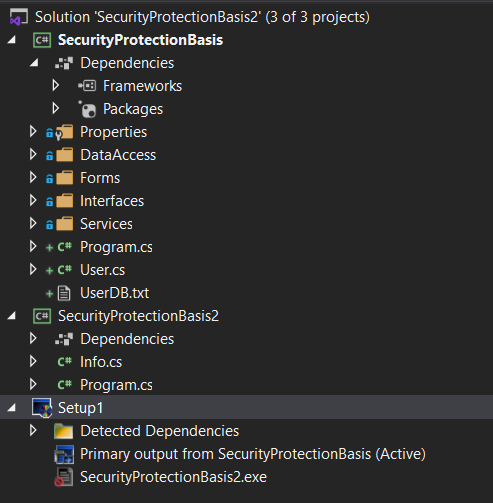


1. Далі були створені методи для підпису даних, їх запису до реєстру та читання з реєстру.

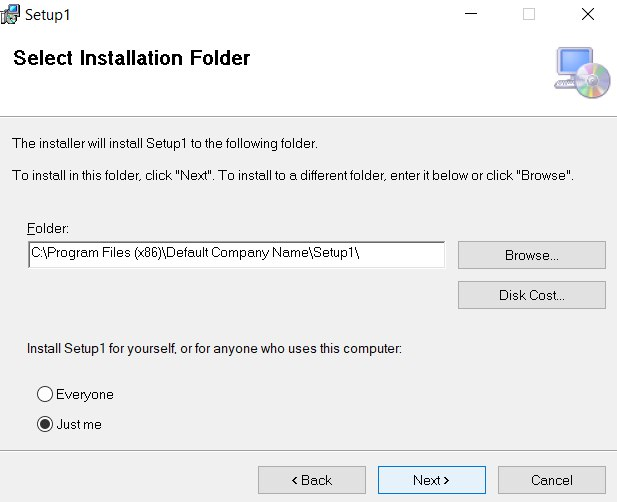




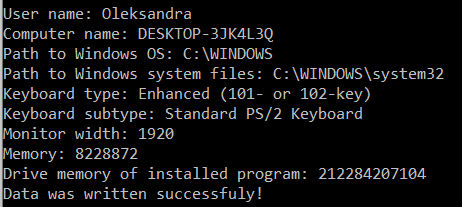
1. Був створений проект Setup1 для налаштування інсталяції програми.



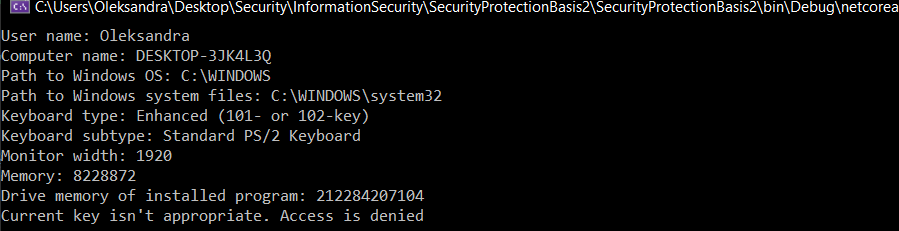
1. Була проведена установка програми.



1. Результат роботи інсталятора з правильним ключем.



1. Результат роботи інсталятора з невірним ключем.

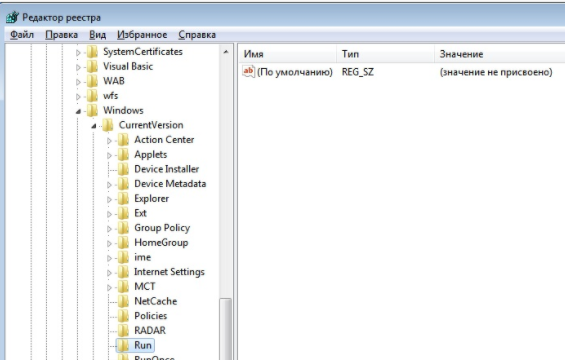


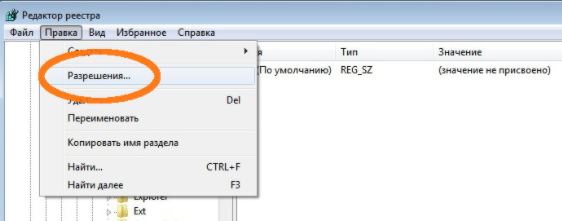
**Відповіді на теоретичні питання**

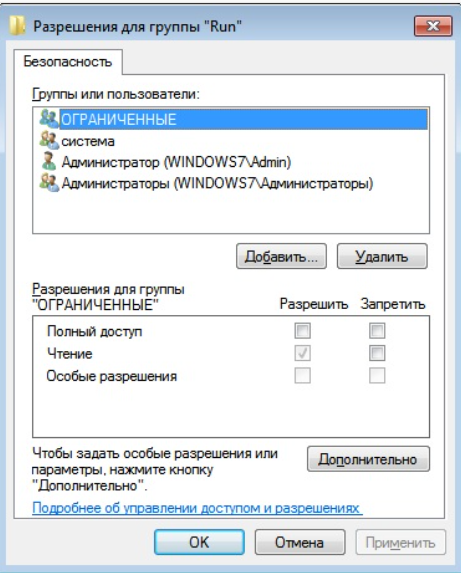
1. Яким чином можливо налаштувати заборону доступу до

визначених ключів реєстра?

Запускаємо редактор реєстру regedit







2. Які параметри забезпечують унікальність інформації, яка

збирається програмою по робочій станції, де вона встановлюється?

SID – ідентифікатор безпеки , що використовується для забезпечення унікальності цієї інформації, так як він призначений для для унікальної ідентифікації учасника безпеки.

3. Що таке хеш-функція. Наведіть приклад.

Функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

Існує декілька методів задання хеш-функції, наприклад, метод середини квадрата, де ключ множиться сам на себе і як індекс ми беремо декілька середніх чисел отриманого значення.

4. Призначення та сфера застосування хеш-функцій.

Хеш-функція дозволяє перетворювати код ключа бази даних на її адресу. Це дає можливість так розміщувати елементи даних в пам'яті, що їх потім нескладно буде знайти. Хеш-функції також широко використовуються при шифруванні.

Аналіз за допомогою хеш-функцій часто використовують для контролю цілісності важливих файлів операційної системи, важливих програм, важливих даних. Контроль може здійснюватися як за необхідності, так і на регулярній основі.

5. Що таке криптопровайдер?

Cryptographic Service Provider (CSP) — це незалежний модуль, що дозволяє здійснювати криптографічні операції в операційних системах Microsoft Windows, управління яким відбувається за допомогою функцій Microsoft CryptoAPI. Модуль реалізує функції розшифрування і зашифрування які потім прикладна програма може використати для створення системи аутентифікації, захищеної електронної пошти чи чогось подібного. Простими словами криптопровайдер виступає посередником між операційною системою та виконавцем криптографічних опрецій(програма чи апаратний комплекс).

6. Які криптографічні функції використані Вами для реалізації

завдань роботи? Наведіть їхні параметри.

CngKey.Create(Cng.Algorithm algorithm) – повертає обьект класу CngKey, що визначає базову функціональність для ключів, використовуваних об'єктами криптографії наступного покоління (CNG).

ECDsaCng.SignData(byte[] data) – генерує підпис певної інформації.

HashAlgorithm.ComputeHash(byte[] buffer) – повертає хеш-значення для певного byte array

**Висновок**

Був створений інсталятор та налаштований процес доступу користувачів до програми. Були досліджені алгоритми шифрування та хеш-функції, а також варіанти їх використання мовою C# на платформі .NET Core.