Загацька Н.О.
асистент кафедри прикладної математики та інформатики,
Житомирський державний університет імені Івана Франка

ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМІВ ШИФРУВАННЯ ЯК СКЛАДОВА САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ З КУРСУ «КРИПТОЛОГІЯ»

На сучасному етапі модернізації системи вищої освіти педагогічний процес має бути спрямований на підготовку фахівця, здатного самостійно вчитися, опановувати нові знання, вдосконалювати практичні навички, розвивати здібності до самоконтролю та самооцінки. У зв'язку з цим особлива роль належить організації самостійної роботи студентів, яка становить від однієї до двох третин загального обсягу навчального часу, відведеного для вивчення конкретної дисципліни.

Самостійна робота є такою, що планується, виконується за завданням, під методичним керівництвом і контролем викладача, але без його безпосередньої

участі [1, с.309]. У цьому контексті варто зазначити, що вміло організована педагогічна взаємодія, а саме надання викладачем чітких інструкцій, рекомендацій, встановлення строків та вимог щодо виконання самостійних завдань, зумовлює становлення студента як свідомої, відповідальної та активної особистості, розвиває його професійний та творчий потенціал. Крім того, важливим чинником успішного результату виконання самостійної роботи є врахування індивідуальних особливостей кожного студента та використання різнорівневих завдань.

В рамках вивчення курсу «Криптологія» самостійна робота студентів передбачає такі види навчальної діяльності:

- опрацювання лекційного матеріалу, додаткової літератури;
- написання рефератів та доповідей;
- підготовка до тестування, контрольної роботи, заліку, іспиту;
- розв'язування математичних задач, що лежать в основі криптографічних перетворень;
- виконання практичних завдань за допомогою спеціалізованого програмного забезпечення;
- програмна реалізація алгоритмів шифрування.

Зважаючи на те, що «Криптологія» є прикладною дисципліною, особлива увага в організації самостійної роботи з цього курсу приділяється виконанню практичних завдань, зокрема програмуванню алгоритмів шифрування. Потужним інструментом, що дозволяє студентам глибше проникнути в суть криптографічних перетворень шляхом їх програмної реалізації в середовищі однієї з мов програмування (C/C++, Pascal, Java) є портал E-Olymp [2]. Даний ресурс було створено на базі Житомирського державного університету імені Івана Франка з метою підготовки обдарованої молоді до дистанційних олімпіад та змагань з програмування.

На сьогоднішній день база E-Olymp налічує тисячі задач, які охоплюють широке коло тем, в тому числі з криптології. Тут можна знайти цікаві задачі, присвячені принципам побудови та функціонування таких криптографічних алгоритмів як шифри Юлія Цезаря, Бекона, Плейфера тощо. Водночас користувачам порталу доступні завдання підвищеної складності, зокрема такі, що ілюструють роботу деяких алгоритмів хешування, а також основні прийоми та методи криптоаналізу.

В результаті самостійного виконання студентами вищеописаних завдань на сайті E-Olymp відбувається закріплення, поглиблення та систематизація теоретичних знань з криптології, розвивається абстрактне та логічне мислення, посилюється мотивація до вивчення дисципліни. Варто зауважити, що усі індивідуальні завдання розподіляються викладачем з урахуванням потенційних можливостей та здібностей студентів.

Як відомо, розв'язання будь-якої прикладної задачі включає етап побудови її математичної моделі. Проектування роботи криптографічних систем на порталі E-Olymp вимагає практичного застосування знань з різних розділів алгебри, комбінаторики, теорії чисел, теорії алгоритмів, теорії ймовірностей і математичної статистики. Це позитивно впливає на активізацію навчально-пізнавальної діяльності студентів, сприяє зміцненню міжпредметних зв'язків математики, криптології та інформатики.

Розглянемо варіант програмної реалізації на сайті E-Olymp дешифрування

повідомлення за алгоритмом Цезаря (рис. 1). Для того щоб отримати початкове повідомлення *p* потрібно кожну літеру деякого зашифрованого тексту *c* замінити на літеру, розташовану в латинському алфавіті на *k* позицій назад. Тобто циклічно зсунути алфавіт на деякий ключ. При досягненні кінця алфавіту відбувається перехід до його початку. Для цього усі операції будемо виконувати за модулем 26: $p_i = (c_i - k)\%26$.

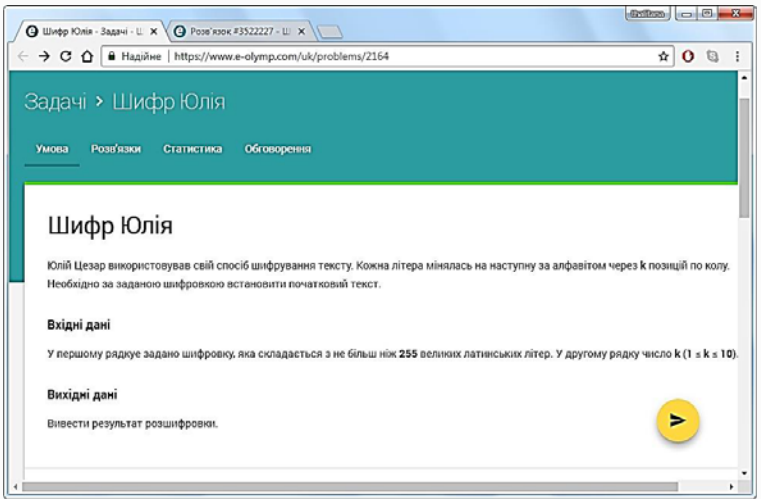

Рис. 1. Вікно з умовою задачі «Шифр Юлія» на порталі E-Olymp

Ідея розв'язання цієї задачі полягає в тому, що кожна літера шифротексту – це певний символ кодової таблиці ASCII. Щоб дешифрувати рядок *c* потрібно від ASCII-значення *i*-го символу відняти значення ключа *k*. Для того, щоб не виходити за межі алфавіту, перед обчисленням остачі від ділення за модулем 26 відніматимемо символ «Z», а потім до отриманого результату додаватимемо символ «Z».

Використовуючи цикл, що повторюється стільки разів, скільки символів в рядку *c*, застосуємо описаний алгоритм до кожної літери c_i (рис. 2). На кожному кроці роботи циклу будемо посимвольно виводити літери початкового повідомлення.

```
#include <iostream>
#include <string>
using namespace std;

int main() {
string c;
getline(cin,c);
int k;
cin>>k;
        for (int i=0; i<c.length(); i++)
            {
             int letter=int(c[i]);
             int p=(letter-k-'Z')%26+'Z';
             cout<<char(p);
            }
        return 0;
}
```

Рис. 2. Варіант розв'язку задачі «Шифр Юлія» на порталі E-Olymp

Крім питання організації самостійної роботи, досить часто виникає проблема її контролю та оцінювання результатів. Система тестів E-Olymp дає

змогу користувачеві надсилати свої розв’язки на перевірку, яка здійснюється за допомогою набору тестів. До кожної задачі є кілька готових вхідних даних, які система по черзі підставляє в код програми. Якщо відповідь збігається з правильною, то тест зараховується і користувач отримує певну кількість балів.

Загалом, в процесі розв’язання криптографічних задач з використанням порталу E-Olymp студенти отримують вміння раціонально організовувати власну діяльність, при цьому самостійно обираючи для себе оптимальний темп, час навчання, місце навчання, необхідний програмний інструментарій тощо. Такий підхід до організації самостійної роботи з курсу «Криптологія» сприяє свідомому засвоєнню майбутніми фахівцями з інформатики навчального матеріалу, забезпечує формування предметних і професійних компетенцій, посилює мотивацію до самонавчання та самовдосконалення.

Список використаних джерел та літератури

1. Кузьмінський А.І. Педагогіка вищої школи: навч. посібник./ А.І. Кузьмінський – К.: Знання, 2005. – 486 с.
2. E-Olymp [Електронний ресурс]. – Режим доступу: https://www.e-olymp.com/