УДК 378.016:512.624.95

Пеньков А.В., Деміденко Б.Р., Коваленко І.В.

ДЕЯКІ ПИТАННЯ МЕТОДИКИ ВИВЧЕННЯ КРИПТОГРАФІЇ У КУРСІ І "БЕЗПЕКА КОМП'ЮТЕРІВ ТА ЗАХИСТ ДАНИХ"

У статті розглядається методику навчання питання захисту інформаційних ресурсів шляхом використання криптографії. Розглянуто як класичні і сучасні методи шифрування, так і використання сучасних комп'ютерних програм як PGP.

Ключові слова: *методика навчання, криптографія, класичні і сучасні методи шифрування, PGP.*

Стрімкий розвиток та розповсюдження інформаційних технологій викликає швидке збільшення проблем та викликів, що пов'язані із захистом інформаційних ресурсів. Тому володіння питаннями захисту інформаційних ресурсів є невіддільною частиною інформаційної культури випускників фізико-математичних факультетів педагогічних університетів. Вивчення теми "Криптологія" є обов'язковою частиною будь якого інформаційного курсу, що пов'язаний із захистом даних та інформаційних ресурсів, що ми бачимо з класичного підручника 70 років минулого століття[1]. Для висвітлення теми в тому обсязі, що надається, слід розкрити такі лінії: історичні найпростіші відомості з криптографії, поняття криптології та криптоаналізу, поняття ключа і криптосистеми та їх класифікація (з секретним ключем, відкритим ключем та криптографічні протоколи) [2,3]. З класичних методів шифрування можна розглядувати шифри перестановки (шифр перестановки Сцималла та таблиці для шифрування), шифри прямої заміни (шифр Цезаря та його модифікації (афінна система підстановок Цезаря та система Цезаря з ключовим словом, ROT13), азбука Морзе, таблиці Трисемуса, біграмний шифр Плейфейра, криптосистема Хілла, система омонімів. Як шифри складної заміни слід розглянути шифр Гронсфельда, шифр Віженера, шифр "Подвійний квадрат Уітстона" та одноразову систему шифрування (разові криптоблокноти). На лабораторному занятті слід розглянути всі види шифру Цезаря як такого, що з одного боку легко зрозумілий, а з іншого боку криптослабкий для подальшого розшифрування за допомогою статистичних таблиць. З цією метою студентами було створено програму "Шифр Цезаря" (текст програми наведено наприкінці статті), за якою зашифровується введений текст шифром Цезаря із довільним зсувом, здійснюється обернена операція та друкується зашифрований (розшифрований) – таким чином легко готуються індивідуальні завдання. До речі, з метою посилення міжпредметних зв'язків в якості додаткового завдання до екзамену студентам може бути запропоновано написати програми, що реалізують наведені вище методи шифрування та інші. Це також може бути завданням до компютерної практики.

При розгляді сучасних та умовно сучасних методів шифрування студенти мають знати їх види (симетричне та асиметричне) та їх реалізації алгоритмами. Для симетричного шифрування ГОСТ28147-89, AES (Rijndael)? Blowfish, DES, TripleDES. Для асиметричного шифрування – алгоритми Діфі-Хеллмана, Ель-Гамаля, RSA.

В якості конкретної програмної реалізації, що має практичне значення, на лабораторному занятті розгляду підлягає всесвітньо відома програма PGP (Pretty Good Privacy) – автор Філ Цімерман, у версіях, які не є платними. Причому розгляду підлягає не лише шифрування (розшифрування) файлів, а й робота з поштою, що шифрується цією програмою, службами миттєвих повідомлень, створення контейнерів та шифрування операційної системи. Особливу увагу слід приділити формуванню в студентів розуміння правильного вилучення файлів (опції WIPE). На самостійне вивчення слід віднести роботу з програмами DriveCrypt, TrueCrypt за матеріалами INTERNET – ресурсів.

Такій підхід до навчання криптології надає студентам не лише теоретичні знання з цієї теми, а й цілком практичні навички забезпечення захисту інформаційних ресурсів засобами сучасних комп'ютерних програм, що мають високий рівень захисту.

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, Mask, Buttons, ExtCtrls, Printers,jpeg, Menus;

type
  TForm1 = class(TForm)
    CheckBox: TCheckBox;
    BitBtn: TBitBtn;
    MaskEdit1: TMaskEdit;
    GroupBox1: TGroupBox;
    GroupBox2: TGroupBox;
    IshMemo: TMemo;
```

```
    ObrMemo: TMemo;
    Label1: TLabel;
    Button2: TButton;
    MainMenu1: TMainMenu;
    faill1: TMenuItem;
    Exit1: TMenuItem;
    Seve1: TMenuItem;
    print1: TMenuItem;
    Button1: TButton;
    Button3: TButton;
    procedure BitBtnClick(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure Exit1Click(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure Button3Click(Sender: TObject);

      private
    { Private declarations }
   public
    { Public declarations }
   end;

    const Buk:array[0..65] of char =
('А','Б','В','Г','Д','Е','Ё','Ж','З','И','Й','К','Л','М','Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ','Ы','Ь','Э','Ю
','Я', 'а','б','в','г','д','е','ё','жс','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ъ','ы','ь','э','ю','я');

  var
   Form1: TForm1;
   b:array[0..65] of char;
   i, j, k: byte;
   s, s2:string;
  implementation

  uses Unit2;

  {$R *.dfm}

  procedure TForm1.BitBtnClick(Sender: TObject);
  begin
  Fori:=0 to 65 do
  begin                    //Формирование нового массива
  b[i]:= Buk[(i+1) mod 66];
   end;

   if CheckBox.Checked = false then begin
     k := StrToInt(MaskEdit1.Text);
     s := IshMemo.Lines.Text;
     for i := 1 to length(s) do
       for j := 0 to 65 do
            if s[i]= ''
     then s[i]:= s[i]
        else
          if s[i] = b[j] then s2 := s2+b[(j+k) mod 66];
     ObrMemo.Lines.Text := s2;
     s2 := '';
   end;

   if CheckBox.Checked = true then begin
     k := StrToInt(MaskEdit1.Text);
     s := IshMemo.Lines.Text;
     for i := 1 to length(s) do
       for j := 0 to 65 do
    if s[i]= ''
     then s[i]:=s[i]
     else
       if s[i] = b[j] then s2 := s2+b[(j-k) mod 66];
     ObrMemo.Lines.Text := s2;
     s2 := '';
   end;

  end;

  procedure TForm1.Button2Click(Sender: TObject);
  var
```

```
 Stroka:System.Text;
 f,g:integer;
begin
//печать в текстовом режиме
 AssignPrn(Stroka);//связь текстовой переменной с принтером
Rewrite(Stroka);
 Printer.Canvas.Font:=IshMemo.Font;
 for f:=0 to IshMemo.Lines.Count-1 do
  Writeln(Stroka,IshMemo.Lines[f]);  //построчнаяпечатьстрок
Writeln(Stroka,'**********************************************************************************************
**********************************');  //построчная печать строк

Printer.Canvas.Font:=ObrMemo.Font;
  for g:=0 to ObrMemo.Lines.Count-1 do
Writeln(Stroka,ObrMemo.Lines[g]);
System.Close(stroka); // разрыв связи после печати
end;

procedure TForm1.Exit1Click(Sender: TObject);
begin
Close;
end;

procedure TForm1. Button1Click (Sender: TObject);
var
f: TextFile; {описфайловоїзмінної}
begin
AssignFile (F, 'text 1. Txt'); {зв'язокфайловоїзмінноїзфайлом}
Rewrite (f); {створити новий файл}
Writeln (f, ishmemo. Text);
writeln(F,'*************************************************************************************');
Writeln (f, obrmemo. Text);
{записатиуфайл}
CloseFile (f); end; {закритифайл}
 procedure TForm1.Button3Click(Sender: TObject);
begin
close;
end;

end.
```

Використані джерела

1. Бауэр Ф.Л., Гнац Р., Хилл У. Информатика. Задачи и решения.– М.: Мир, 1978.– 360 с.
2. Бойцев О. Защити свой компьютер от вирусов и хакеров. –СПб.: Питер, 2008.– 288 с.
3. Жельников В. Криптография от папируса до компьютера.– М.: ADF, 1996.– 335 с.

Penkov A.V., DemidenkoB.R., KovalenkoI.V.

SOME PROBLEMS OF METHODS OF STUDYOF CRYPTOGRAPHY IN THE COURSE "COMPUTER SECURITY AND PROTECTION OFINFORMATION RESOURCES"

The article deals with methods of study of problems of information resources protection by the use of cryptography. Both classical and modern methods of encryption and usage of modern software such as PGP are observed.

Key words: *methods of study, cryptography, classical and modern methods of encryption, PGP.*

Стаття надійшла до редакції 12.08.2013 р.