УДК 378.016:512.624.95

Пеньков А.В.

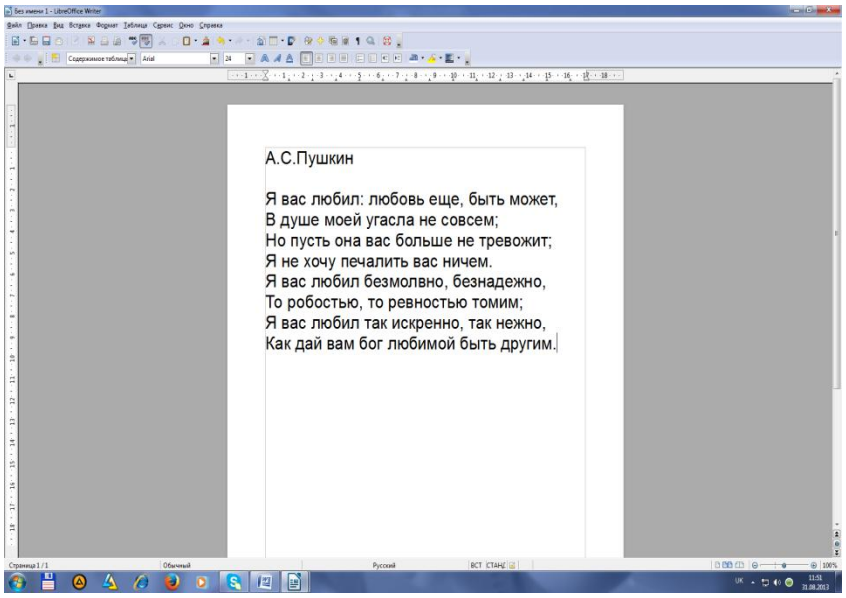
ДЕЯКІ ПИТАННЯ МЕТОДИКИ ВИВЧЕННЯ СТЕНОГРАФІЇ У КУРСІ "БЕЗПЕКА КОМП'ЮТЕРІВ ТА ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ"

У статті розглядається методика навчання питання захисту інформаційних ресурсів шляхом використання такого розділу криптографії як стеганографія. Розглянуто як наочні штучні способи, так і використання сучасних комп'ютерних стегосистем як STEGANOS.

Ключові слова: *методика навчання, криптографія, стеганографія, штучні способи, комп'ютерні стегосистеми, STEGANOS.*

Вивчення теми "Криптологія" є обов'язковою частиною будь якого інформаційного курсу, що пов'язаний із захистом інформаційних ресурсів [1]. Але до умовно класичного змісту теми слід додати розгляд такого цікавого сучасного способу шифрування, як стеганографія, зокрема комп'ютерна.

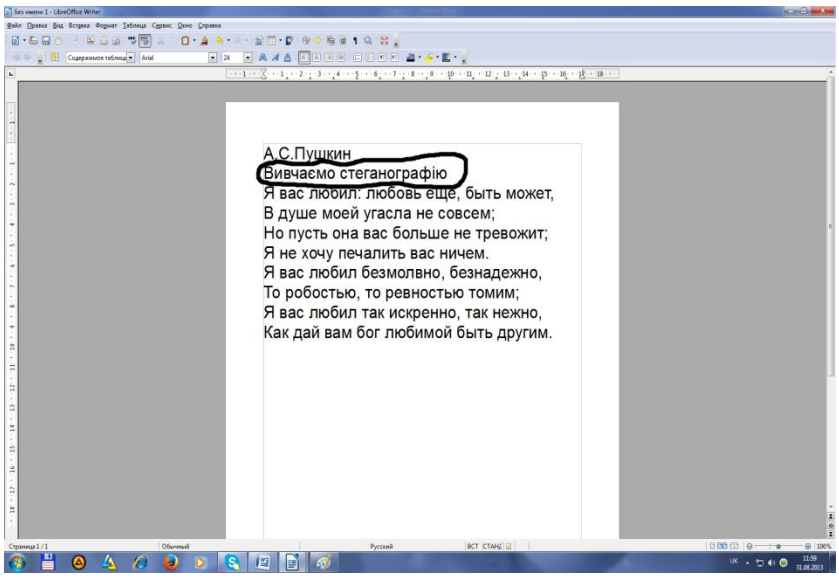
Шифрування файлу-повідомлення сучасними програмними засобами такими як PGP, FileCrypt тощо дописує до його імені додаткове розширення файлу – відповідно .pgp, fcrpt тощо. Перехоплення такого повідомлення викликає підозру про його зміст. Звичайно додаткового розширення можна позбутися, навіть у налагодженнях програми, але перехоплений файл не буде відповідати структурі, яка визначається його розширенням. Виникає цілком слушне запитання – чи не можна приховувати сам факт наявності такого таємного повідомлення. Виявляється, що можна. Саме для цього і застосовують стеганографію. Отже, стеганографія – це наука про сховане передавання інформації шляхом збереження у таємниці власно факту цього передавання. Розглядаючи з студентами використання стеганографії, для початку можна запропонувати відкрити певний документ із заздалегідь набраним текстом та поставити завдання: знайти у запропонованому тексті сховане таємне повідомлення, якщо воно є (Мал.1)



Мал. 1

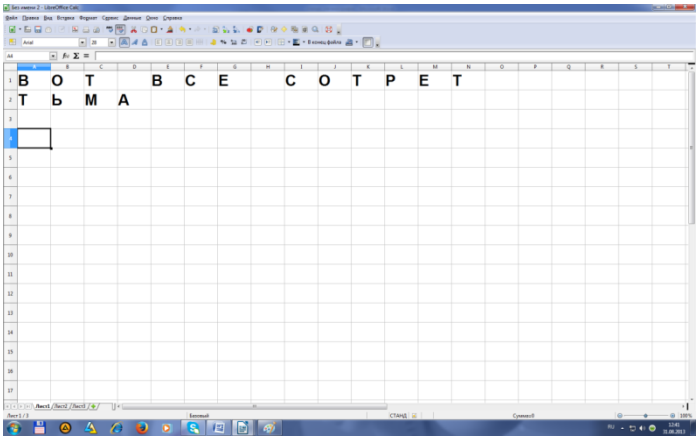
Обговорення питання зазвичай призводить до думки, що слід обирати лише певні літери тексту за певним правилом. Цю думку слід заохотити та розповісти студентам, що таке акровірш (телевірш, мезовірш) та розповісти про його модифікації. Але насправді в даному випадку все набагато простіше – таємне повідомлення написано білим по білому, тому шляхом виділення усього тексту та обрання чорного шрифту для всього тексту побачимо таке (Мал. 2).

Тут можна згадати про існування спеціальних невидимих чорнил, що використовували різноманітні розвідки, народні "революційні" (у сенсі діяльності революціонерів) методи стеганографії молоком на папері та сучасні "дитячі" способи письма ультрафіолетовими маркерами з наступним читанням у ультрафіолетовому світлі (цей простий спосіб використовує навіть ДАІ для запобігання угону автівок).

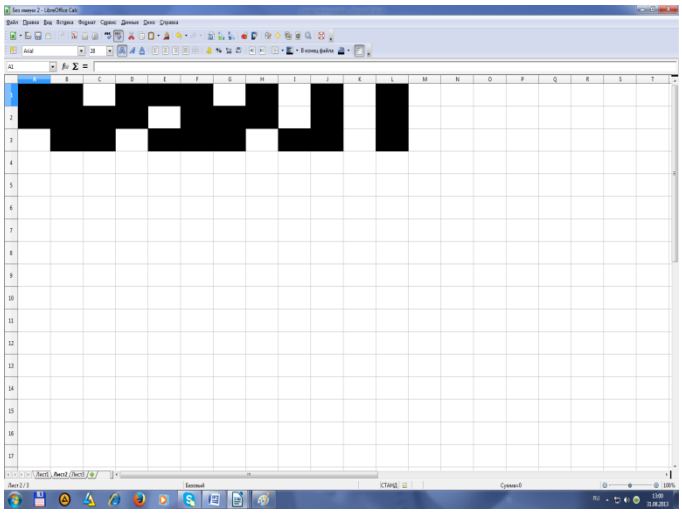


Мал. 2

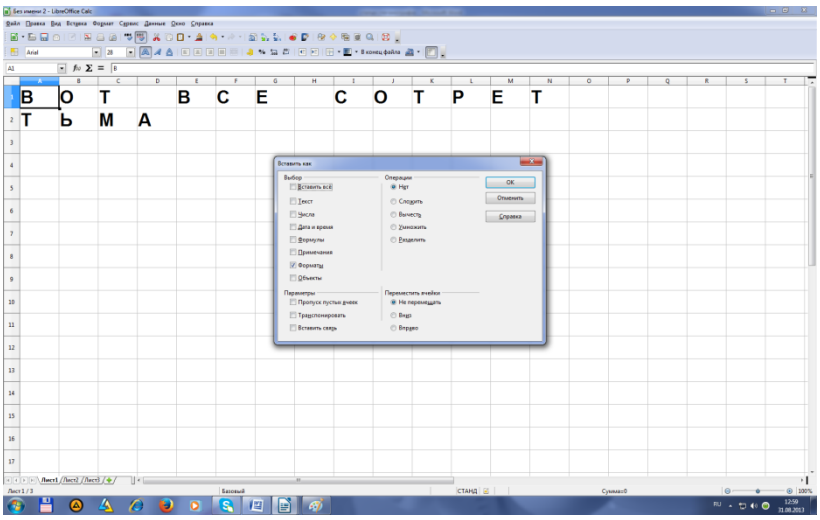
Далі можна розповісти про таку просту програмну реалізацію модифікованого акровірша, коли в повідомленні слід читати літери за певним законом. Раніше повідомлення писались на аркуші паперу у клітинку, а для розшифрування використовували такий же аркуш, де певні клітинки були вирізані – таємне повідомлення отримували шляхом накладання аркушів. Це можна продемонструвати таким простим прикладом: повідомлення створюється у електронній таблиці на Аркуші1 (Мал. 3), правило для розшифрування (ключ) на Аркуші 2 (Мал. 4), для отримання таємного повідомлення слід зробити копіювання формату з Аркушу 2 на Аркуш1 (Мал. 5, 6):



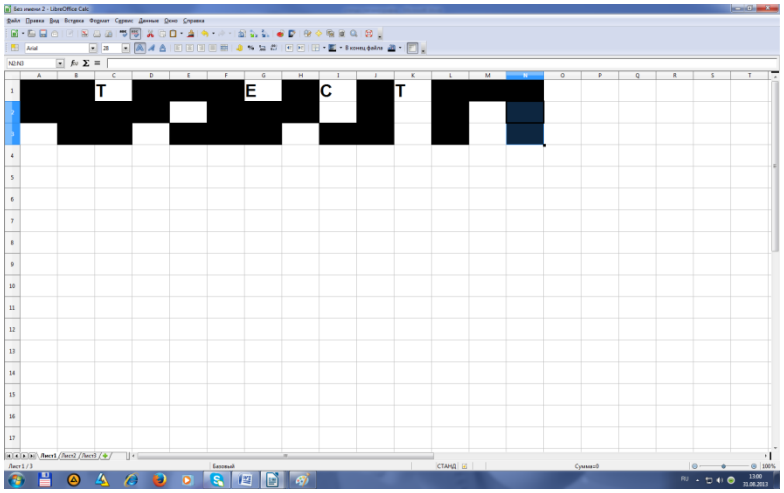
Мал. 3



Мал. 4

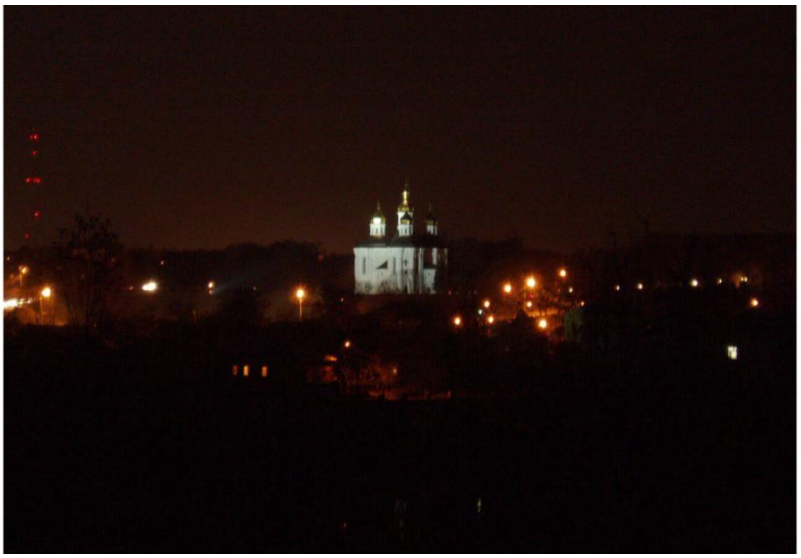


Мал. 5

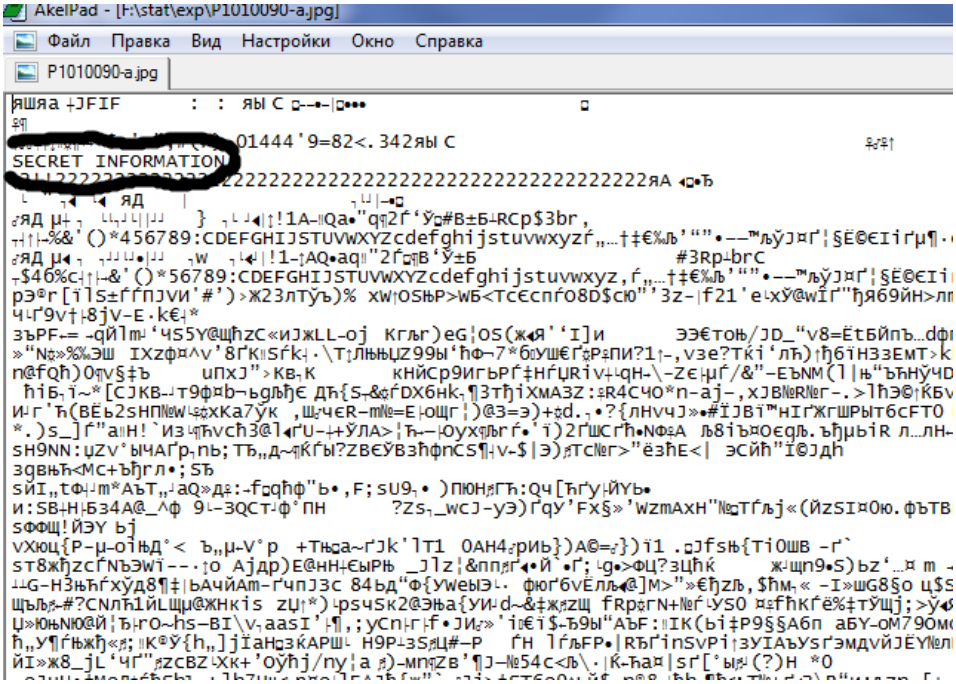


Мал. 6

Далі можна перейти до наступного етапу розгляду стеганографії. Студентам слід запропонувати подивиться на фото нічного Чернігова (Мал. 7), А потім продивиться зміст цього фото (JPG-файлу) в тектовому редакторі (наприклад у редакторі будь-якого файлового менеджера) та показати, що файл має таємне повідомлення "SECRETINFORMATION" (Мал. 8)

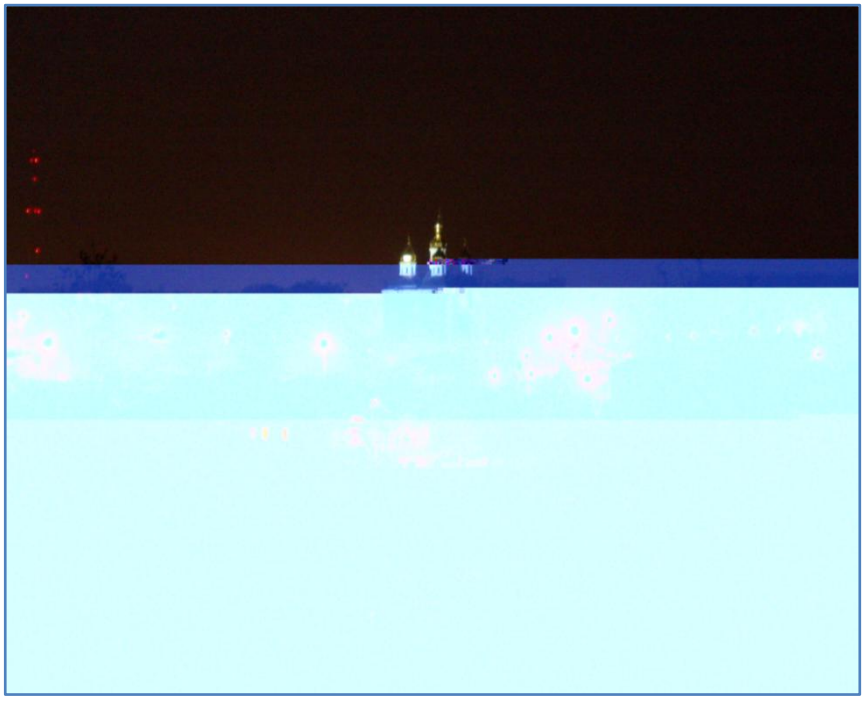


Мал. 7



Мал. 8

Після цього слід показати, що вставляння всередину початкового бінарного файлу меншого повідомлення "TEST", але в іншому місці призводить до спотворення фотографії (Мал. 9).



Мал. 9

Таким чином робиться висновок про те, що структура файлу має значення для вписування таємних повідомлень. Так відбувається перехід до поняття маркерів мультимедійних файлів – цю тему слід віднести

на самостійне опрацювання (для jpg, bmp, wav і mp3 файлів). Слід зазначити, що неможливо знаходити маркери в такий спосіб, як відбувався перегляд змісту бінарного файлу вище, тут слід використовувати інші редактори, наприклад, WINHEX16. Після цього слід показати можливість ручного внесення таємного повідомлення до bmp, wav і mp3 файлів з наступними спробами побачити або почути різницю між початковим та зміненим файлом. Таким чином, студенти мають розуміти, що спілкування у соцмережах з демонстрацією фотографій та викладанням музичних та відео файлів може бути насправді прихованим каналом обміну таємними повідомленнями. Далі можна перейти до вивчення нетривіальних способів приховування повідомлень з розглядом відповідних програмних засобів.

Слід дати означення стеганографії, повідомити про її типи, ввести поняття стегосистеми, вимог до неї, типи стегосистем за ключом, поняття контейнеру, методи приховування даних у контейнері (за властивостями тексту, за структурою файлів, за надлишковістю аудіовізуальних файлів), типи атак на стегосистеми. Студенти мають розуміти, що співвідношення обсягу таємного повідомлення до обсягу контейнера має суттєве значення. Не можна ховати повідомлення у 0.5 мб у файлі обсягом 2 мб, якою б професійною програмою це не здійснювати. Спотворення буде занадто наочним, навіть 10% таємних данихє критичним розміром. З цього випливає два висновки – стегосистема має попередньо стиснути таємне повідомлення та зашифрувати його стійким алгоритмом (Blowfish, Idea32, TripleDes тощо), і тільки потім занести повідомлення до контейнеру.

Слід зазначити, що стегометоди використовуються для внесення певних даних до файлів-програм, фотографій тощо також з метою охорони авторського права – так звані цифрові водяні знаки. До речі, режим цифрових водяних знаків є наявним у певних системах відеоспостереження – для унеможливлення підробки відеофайлів.

Як приклад професійної реалізації стегосистем слід навести студентам такі програми як STEGANOS і DriveCrypt (ознайомитися з ними можна відповідно на сайтах www.steganos.com та www.drivecrypt.com, за описами в Інтернеті – програми ліцензійні) та програму Stegdetect (http://www.outguess.org/detection.php)– для пошуку зашифрованих стегоповідомлень.

На практичну роботу слід винести роботу із вільнопоширюваними ПЗ Fox Secret і ImageSpyer. Причому сховані у стегоконтейнері мають бути не тільки текстові повідомлення (текстові документи), а також файли інших типів – xls, gif тощо.

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.

SOME PROBLEMS OF METHODS OF STUDY OFSTEGANOGRAPHY 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 such part of cryptography as steganography. Both visual artificial methods and usage of modern computer stegosystems such as STEGANOS are observed.

Key words: *methods of study, cryptography, steganography, artificial methods, computer stegosystems, STEGANOS.*

Стаття надійшла до редакції 12.08.2013 р.