

## ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В АУДІОФАЙЛАХ

Руєва А. В.

Національний аерокосмічний університет ім. М. Е. Жуковського  
«Харківський авіаційний інститут»  
Науковий керівник Певнєв В. Я.

**Актуальність.** Розвиток інформаційних технологій спричинило різке збільшення можливостей незаконного доступу до інформації. У зв'язку із цим на перший план виходить інформаційна безпека, яка є складовою безпеки будь-якої держави. Одночасно зростає роль кібербезпеки. Використання комп'ютерної техніки дозволяє зробити прорив у багатьох галузях науки та техніки, медицині, виробництві та інших галузях. Водночас зростають загрози від незаконного отримання інформації, її зміни. Існуючі способи забезпечення конфіденційності, цілісності та доступності не здатні повністю усунути загрози для інформації, що передається. Багато фахівців вважають основним способом вирішення більшості завдань, що виникають при забезпеченні інформаційної безпеки, використання криптографії [1].

Одним із найбільш перспективним методом забезпечення конфіденційності та цілісності інформації є стеганографія, яка приховує сам факт передачі інформації [2]. Як контейнер, в якому розміщується повідомлення, що передається, можуть використовуватися текстові, графічні, аудіо- та відеофайли. Надійність такого способу передачі зростає, коли одночасно використовуються криптографічні та стеганографічні методи приховування інформації [3].

**Метою** даної роботи є дослідження можливостей приховування інформації в аудіофайлах, розробка блоків одно- та двобітового приховування.

**Основні положення.** У доповіді наведені наступні методи приховування інформації в аудіофайлах: вбудовування з розширенням спектра, вбудовування за рахунок модифікації фази аудіосигналу, вбудовування за рахунок зміни часу затримки echo-сигналу, вбудовування інформації в найменший біт. Порівняльний аналіз цих методів показав, що кожен з них має свої недоліки та переваги, а методи фазового кодування та луна-метод є найкращими для приховування даних (зберігають якість аудіофайлу, стійкі до модифікацій). Але на

відміну від методу фазового кодування, луна-метод є не так глибоко вивченим та однозначним як фазовий[4]. В доповіді представлено алгоритм з розробкою блоків побітового та двобітового приховування та визначено «формуючі величини» для луна-методу. Також було показано можливості луна методу шляхом проведення експериментів з різними контейнерами та різною довжиною приховуваної інформації. Результати експериментів демонструються за допомогою аудіофайлів.

**Висновки.** В доповіді було проаналізовано можливість вбудовування інформації луна-методом з використання блоків інформаційного приховування. Відмінні риси луна-методу дозволяють приховувати інформацію в аудіофайли, переслідуючи різні цілі, такі як: захист авторських прав, прав інтелектуальної власності або конфіденційних даних а також захист від НСД. Для цього в роботі було показано різні модифікації алгоритму. Було визначено, що ефективність використання двобітового блоку зростає з і збільшенням самого приховуваного тексту.

#### **Список літератури**

1. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации: навч.-метод. посіб. Мінськ : БДТУ, 2016. 220 с.
2. Певнев В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.
3. Pevnev V., Voikov Yu. Research and Prototyping Methods of Steganography Using Mosaic. *Advanced Information Systems*. 2020. Vol. 4, No.2. P.137-141
4. Singh P. A Comparative Study of Audio Steganography Techniques. *IRJET*. 2016. Том 3, Випуск 4. с. 580-585.

#### **Відомості про авторів**

Руєва Анастасія Володимирівна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-25-82-148, a.ruieva@student.csn.khai.edu

Певнев Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu