# ДОСЛІДЖЕННЯ НАДІЙНОСТІ АЛГОРИТМІВ ЗАХИСТУ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ.

Цалімов М.Г., Кушніренко О.А.

Науковий керівник – доц. каф. “Радіотехнічні системи”, канд. техн. наук Садченко А.В.

Одним із ефективних способів захисту авторських прав є використання алгоритму електронного цифрового підпису (ЕЦП) [1,2].

ЕЦП дозволяє підтвердити той факт, що електронна інформація дійсно належить даному авторові. Електронна інформація в навчальних закладах може бути представлена у вигляді конспекту лекцій, методичних вказівок, навчальних посібників і інших документів. Як об'єкт аналізу обрано найпоширеніші алгоритми ЕЦП - DSA та RSA, складність злому яких заснована на рішенні завдання дискретного логарифмування в простому полі Галуа [1].

Незважаючи на численні достоїнства ЕЦП, її головна уразливість - принципова можливість підробки.

Один з основних недоліків алгоритмів ЕЦП - передбачуваність випадкових чисел, які виробляє генератор секретних ключів (при кожному виконанні алгоритму генерації випадкових чисел одержимо той же самий список випадкових чисел).

Для підвищення крипостійкості алгоритмів ЕЦП пропонується використовувати апаратний генератор випадкових чисел із зовнішньою ентропією. Як джерело зовнішньої ентропії обраний шум звукової карти Realtek ALC655.

Проведені дослідження шумових характеристик АЦП звукової карти ALC655 показали, що шум молодших розрядів має Гаусовський закон розподілу ймовірностей вибірок. Після застосування функціонального перетворення до отриманого масиву вибірок вдалось отримати рівномірний закон розподілу ймовірностей [2].

Запропонований підхід до формування секретних ключів дозволяє спростити алгоритм цифрового підпису за рахунок використання дійсно випадкових чисел і ключів меншої довжини в порівнянні з конгруентним алгоритмом генерацій ключів [1].

1. Введение в криптографию / Под общей ред. В.В. Ященко // СПб.: Питер, 2001.

2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2004.