МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

IMA :: 2017

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 17–21 квітня 2017 року)

Суми
Сумський державний університет
2017

Аналіз стійкості криптографічних систем

Химченко Ю.В., *студент*
Сумський державний університет, м. Суми

В наш час, еру інформаційного суспільства, питання стійкості криптографічних систем як ніколи актуальне. Задля безпечного обміну інформацією необхідні стійкі криптографічні системи захисту інформації.

В праці Клода Шенона було доведено існування абсолютно стійких алгоритмів шифрування та визначені вимоги до систем такого роду:

- Ключ генерується для кожного повідомлення;
- Ключ статистично надійний;
- Довжина ключа дорівнює або більша за довжину повідомлення.

Стійкість даних систем не залежить від обчислювальної потужності атакуючої сторони, але через міркування вартості і зручності користування використання даних систем обмежене.

На практиці використовують практично стійкі або обчислювально стійкі системи захисту інформації, які залежать від потужностей дешифратора.

Стійкість практично або обчислювально стійких систем оцінюється виключно на певний момент часу двома критеріями:

- Обчислювальна складність повного перебору;
- Відомі на даний момент уразливості та їх вплив на обчислювальну складність.

Для кожного конкретного випадку можуть існувати додаткові критерії оцінки стійкості системи.

Керівник: Козлова І.І., *старший викладач*