УДК 004.056.55
**І.І. Рій, Є.В. Тиш, к.т.н.**
Тернопільський національний технічний університет імені Івана Пулюя, Україна

# ПОРІВНЯЛЬНИЙ АНАЛІЗ ХАОТИЧНИХ І КЛАСИЧНИХ МЕТОДІВ ШИФРУВАННЯ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ ЕНТРОПІЇ

**I.I. Rii, Ie.V.Tysh, Ph. D.**

# COMPARATIVE ANALYSIS OF CHAOTIC AND CLASSIC ENCRYPTION METHODS FROM THE POINT OF VIEW OF INFORMATION ENTROPY

Інформаційна ентропія є ключовим показником ефективності криптографічних методів, оскільки характеризує рівень непередбачуваності та статистичної рівномірності зашифрованих даних. Хаотичні системи завдяки чутливості до початкових умов, нелінійності та неперіодичності демонструють високий потенціал у формуванні перетворень із підвищеною ентропійністю. На відміну від класичних алгоритмів, де випадковість створюється детермінованими структурними елементами, хаотичні мапи формують нерегулярні траєкторії та послідовності, близькі до максимальної щільності інформації.

Сучасні дослідження показують (див.табл.1), що коректно реалізовані хаотичні алгоритми здатні забезпечувати ентропію шифротексту на рівні 7.98–7.999 біт для 8-бітних даних, що близько до ідеальної випадковості. Класичні криптосистеми (AES, Twofish, ChaCha20) демонструють подібні значення, однак їх ентропійні показники суттєво залежать від режиму шифрування та організації блоків, що визначає різницю у потенційній стійкості до статистичних атак.

Таблиця 1 – Порівняння хаотичних та класичних методів шифрування

| Критерій | Хаотичні методи | Класичні методи |
|---|---|---|
| Середня ентропія шифротексту | 7.95–7.999 біт/симв. | 7.90–7.999 біт/симв. (залежно від режиму) |
| Джерело випадковості | Хаотичні динамічні мапи | Криптоперетворення на основі підстановок і перестановок |
| Чутливість до початкових вимог | Висока | Низька |
| Стійкість до статичного аналізу | Середня  залежить від моделі хаосу) | Висока |
| Чутливість до параметрів | Висока (критичні параметри хаосу) | Низька |

Попри високий ентропійний потенціал хаотичних методів, їх практичне застосування вимагає ретельного вибору параметрів, оскільки переходи між регулярним та хаотичним режимами можуть знижувати криптостійкість. Класичні ж алгоритми, навпаки, забезпечують стабільність та перевірену відповідність стандартам, але вимагають складної структурної організації для досягнення високої ентропії.

Таким чином, обидва підходи здатні забезпечувати високий рівень ентропії шифрованих даних, однак хаотичні системи мають потенціал перевищувати класичні методи за рахунок природної нелінійності та випадковості, що відкриває можливості для створення нових криптографічних примітивів.