УДК 004.056.55: 004.382
І. Рій; Є. Тиш, к. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ПОБУДОВИ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ХАОТИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ДЛЯ СУЧАСНИХ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ

UDC 004.056.55: 004.382
I. Rii; Ie. Tysh, PhD.

METHODS FOR CONSTRUCTING AND COMPARATIVE ANALYSIS OF CHAOTIC ENCRYPTION ALGORITHMS FOR MODERN COMPUTERIZED SYSTEMS

Сучасні комп'ютеризовані системи працюють в умовах стрімкого зростання обсягів да них та ускладнення кіберзагроз, що потребує використання більш ефективних методів захисту інформації. Класичні криптографічні підходи не завжди забезпечують необхідну стійкість та продуктивність, особливо у високошвидкісних або розподілених середовищах. Тому все більшої актуальності набувають хаотичні динамічні системи, які завдяки непередбачуваності, ергодичності та чутливості до початкових параметрів здатні підвищувати рівень безпеки у цифрових платформах.

Хаотичні алгоритми шифрування застосовують різні математичні моделі хаосу, зокрема, логістичну мапу, відображення Генона, тентову та синусну мапи, а також багатовимірні атрактори Лоренца (див. табл. 1). Ці системи генерують послідовності, близькі до випадкового шуму, що дозволяє формувати ключі, підстановки та перестановки з високою ентропією. У комп'ютеризованих системах процес реалізації хаотичного шифрування зазвичай включає ініціалізацію хаотичної моделі, генерацію псевдовипадкових послідовностей та їх подальше використання в операціях захисту даних.

Таблиця 1. Порівняння ключових властивостей базових хаотичних карт

Хаотична мапа	Переваги	Недоліки
Логістична	Проста реалізація, висока ентропія	Може втрачати хаос при певних параметрах
Тентова	Лінійність, рівномірний розподіл	Чутлива до обчислювальних похибок
Генона	Створює складні траєкторії	Вища обчислювальна вартість
Лоренца	Сильна хаотичність, тривимірність	Потребує точних обчислень та апаратної оптимізації

В основі сучасних методів хаотичного шифрування лежить використання як поодиноких, так і комбінованих хаотичних відображень, часто з адаптивним керуванням параметрами в реальному часі. Найбільш перспективним підходом є побудова гібридних криптосистем, де хаос інтегрується з класичними алгоритмами (такими як AES, мережі Фейстеля, S/P-блоки). Така синергія дозволяє підвищити ентропію вихідного сигналу та мінімізувати кореляції, суттєво посилюючи криптостійкість без критичного збільшення обчислювальної складності.

Розвиток хаотичних криптосистем є стратегічно важливим для безпеки сучасних комп'ютеризованих інфраструктур. Завдяки високій непередбачуваності та стійкості до криптоаналізу, ці алгоритми мають потенціал стати стандартом захисту даних у майбутніх цифрових екосистемах від периферійних обчислень до хмарних платформ.