**КРИПТОСИСТЕМА НА ОСНОВІ ХАОТИЧНИХ АТТРАКТОРІВ ДЛЯ ШИФРУВАННЯ КОЛЬОРОВИХ ЗОБРАЖЕНЬ**

**Білозьоров В. Є.,** belozvye2017@gmail.com,

**Гук Н. А.,** [NatalyGuk29@gmail.com](mailto:NatalyGuk29@gmail.com),

**Єгошкін Д. І.,** K[nightDanila@i.ua](mailto:KnightDanila@i.ua)

*Дніпровський національний університет імені Олеся Гончара*

Стрімкий розвиток обчислювальних технологій та алгоритмів шифрування зробив захист конфіденційних даних та безпечну комунікацію невід'ємною складовою сучасного суспільства [1]. Із зростанням обчислювальних потужностей, включаючи квантові обчислення, традиційні методи шифрування стають вразливими, що сприяє розвитку інноваційних криптографічних технологій.

Стандартні криптосистеми AES, RSA та ECC, разом із апаратними модулями, такими як TPM (Trusted Platform Module) та HSM (Hardware Security Module), та Apple Secure Enclave забезпечують надійний захист [2,3]. Однак зростання обчислювальних потужностей призводить до збільшення попиту на надійні методи шифрування. А саме пропонується розглянути потенціал хаотичних і гіперхаотичних систем для підвищення криптографічної безпеки при шифруванні зображень.

Збільшення довжини ключа у криптографічних алгоритмах підвищує стійкість шифрування до різних атак. Це забезпечує захист від атак грубої сили (brute-force) і методів криптоаналізу та враховує майбутнє зростання обчислювальної потужності [4]. Довший ключ збільшує кількість можливих комбінацій, що значно ускладнює підбір методом грубої сили. Однак розвиток квантових обчислень робить класичні алгоритми вразливими, і хоча збільшення довжини ключа може забезпечити додатковий захист, вже розробляються квантово-стійкі алгоритми.

Квантово-стійкі алгоритми, також відомі як постквантова криптографія (PQC). Галузь PQC зосереджена на створенні алгоритмів, що залишаються безпечними навіть за наявності квантових комп’ютерів. До таких підходів належать криптографічні схеми на основі мультиваріантності, криптографія на ізогенії суперсингулярних еліптичних кривих, генерація ключів на основі хаотичних атракторів та шифрування на основі гіперхаотичних атракторів [4, 5, 6, 7]. Ці методи демонструють високу стійкість до квантових атак, що робить їх перспективним вибором для майбутніх систем захисту даних. Атрактори застосовуються в криптографії для захисту від квантових атак завдяки їх здатності генерувати складні, непередбачувані траєкторії, що ускладнює аналіз даних. У контексті стійкості до квантових атак атрактори використовуються для створення ключів, криптографічних послідовностей і шифрувальних схем, які мають хаотичність і непередбачуваність.

У цій роботі області тяжіння атрактору застосовуються для генерації шифрувальних ключів, оскільки вона визначає регіон початкових умов, що ведуть до генерування траєкторій у динамічній системі [8]. Ці траєкторії використані для створення хаотичних послідовностей, які породжують високий рівень непередбачуваності та використовуються у подальшому шифруванні данних.

**Бібліографічні посилання:**

1. M. Yang, N. Bourbakis, L. Shujun, Dataimage Video Encryption, Potentials, 23, (2004), 28-34.
2. D. R. Stinson, M. B. Paterson, Cryptography: Theory and Practice, 4th ed., CRC Press, 2019, ISBN: 978-1-1381-9701-5.
3. J. Katz, Y. Lindell, Introduction to Modern Cryptography, Second Edition, CRC Press, Taylor & Francis Group, 2015, ISBN-13: 978-1-4665-7027-6.
4. M. Barbeau, Quantum data communication protection with the quantum permutation pad block cipher in counter mode and Clifford operators, F1000Research, 12, (2023), 1123. 10.12688/f1000research.140027.1.
5. O. Al-Hazaimeh, M. Al-Jamal, N. Alhindawi, A. Omari, Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys, Neural Computing and Applications, 31, (2019), 1-11. 10.1007/s00521-017-3195-1.
6. B. Zhang, L. Liu, Chaos-Based Image Encryption: Review, Application, and Challenges, Mathematics, 11, no. 11, (2023), 2585. <https://doi.org/10.3390/math11112585>.
7. S. C. Koduru, V. Chandrasekaran, Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption, 2008 IEEE International Conference on Communications and Information Technology Workshops, 260-263. 10.1109/CIT.2008.Workshops.33.
8. G. Datseris, A. Wagemakers, Effortless estimation of basins of attraction, Chaos: An Interdisciplinary Journal of Nonlinear Science, 32, no. 2, (2022), 023104. 10.1063/5.0076568.