УДК 004.056.55:519.876.5:004.89 DOI: 10.31673/2412-4338.2025.048916

Складанний Павло Миколайович
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0002-7775-6039

Гулак Геннадій Миколайович
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0001-9131-9233

Костюк Юлія Володимирівна
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0001-5423-0985

ГЕНЕРАТОР ХАОТИЧНИХ ЧИСЕЛ ІЗ НЕЧІТКИМ КЕРУВАННЯМ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ ІЗ ДИНАМІЧНОЮ ДОВІРОЮ

Анотація. *У статті запропоновано модель генератора хаотичних чисел (Chaotic Random Number Generator, CRNG) з елементами нечіткого керування, орієнтовану на адаптивне регулювання параметрів хаотичної карти залежно від динамічного рівня довіри системи. Такий підхід дає змогу поєднати криптографічну стійкість хаотичних процесів із гнучкістю нечітких регуляторів, що підвищує ентропійність і стійкість генератора до атак відновлення стану. Запропоновано математичну модель на основі карти Чебишева другого роду, у якій коефіцієнт хаотичності та збурення визначаються нечітким регулятором типу Мамдані залежно від поточного рівня довіри (trust score). Формалізовано процедуру фазифікації, побудовано базу правил і дефазифікації з урахуванням поведінкових і контекстних параметрів. Проведено моделювання роботи генератора, яке показало здатність системи самостійно коригувати рівень хаотичності при зміні довіри та підтримувати високу ентропію вихідної послідовності. Для підтвердження ефективності проведено тестування за методиками NIST SP 800-22 та Dieharder, що засвідчило проходження понад 98 % тестів та підвищення ентропії на 2–3 % порівняно з класичними CSPRNG. Результати доводять доцільність використання нечіткої логіки для регулювання параметрів хаотичних генераторів у криптосистемах із динамічною довірою, Zero Trust-архітектурах та системах багатофакторної аутентифікації. Отримані висновки свідчать про перспективність подальшої апаратної реалізації моделі на FPGA та інтеграції у засоби адаптивного управління безпекою.*

Ключові слова: *хаотичний генератор випадкових чисел, нечітка логіка, криптографічна стійкість, динамічна довіра, керування ентропією, криптографічні системи, Zero Trust, адаптивна безпека, карта Чебишева.*

Pavlo Skladannyi
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0002-7775-6039

Hennadii Hulak
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0001-9131-9233

Yuliia Kostiuk
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0001-5423-0985

CHAOTIC RANDOM NUMBER GENERATOR WITH FUZZY CONTROL FOR CRYPTOGRAPHIC SYSTEMS WITH DYNAMIC TRUST

Abstract. *The paper proposes a model of a Chaotic Random Number Generator (CRNG) with fuzzy control elements, designed for adaptive adjustment of chaotic map parameters according to the dynamic trust level of the system. This approach combines the cryptographic robustness of chaotic processes with the flexibility of fuzzy regulators, enhancing the entropy and resistance of the generator against state-recovery attacks. A mathematical model based on the second-order Chebyshev map is developed, where the chaoticity coefficient and disturbance are determined by a Mamdani-type fuzzy controller depending on the current trust score. The fuzzification procedure, rule base, and defuzzification process are formalized considering behavioral and contextual parameters. Simulation of the generator*

demonstrated the system's ability to autonomously adjust its chaoticity level as trust varies and to maintain high entropy of the output sequence. To confirm the effectiveness, testing was carried out using the NIST SP 800-22 and Dieharder suites, showing over 98% test pass rates and a 2–3% entropy increase compared to classical CSPRNGs. The results confirm the feasibility of applying fuzzy logic for regulating the parameters of chaotic generators in cryptographic systems with dynamic trust, Zero Trust architectures, and multi-factor authentication mechanisms. The findings indicate the potential for further hardware implementation of the model on FPGA and its integration into adaptive security management tools.

Keywords: *chaotic random number generator, fuzzy logic, cryptographic strength, dynamic trust, entropy control, cryptographic systems, Zero Trust, adaptive security, Chebyshev map.*

1. Вступ.

Випадковість є одним із фундаментальних ресурсів сучасних криптографічних систем, оскільки визначає їхню стійкість до атак, надійність процесів аутентифікації та безпеку протоколів шифрування й обміну ключами [1-2]. У межах концепцій Zero Trust і Risk-Based Authentication генератори випадкових чисел мають не лише забезпечувати криптографічну випадковість, а й адаптуватися до змінного рівня довіри, поведінкових факторів і контексту ризику. Класичні генератори псевдовипадкових чисел (PRNG, CSPRNG) є статичними системами з фіксованими параметрами, що обмежує їх ефективність у середовищах із динамічними умовами безпеки. Відсутність механізмів контекстного самоналаштування призводить до зниження ентропії та потенційної передбачуваності вихідних послідовностей.

Хаотичні системи, на відміну від традиційних підходів, поєднують математичну простоту з високою ентропійністю та властивістю детермінованої непередбачуваності. Їх ергодичність, чутливість до початкових умов і складна фазова структура роблять їх привабливими для криптографічного застосування. Однак навіть хаотичні карти, як-от Чебишева або логістична, мають суттєве обмеження − залежність рівня хаотичності від фіксованих параметрів, що унеможливлює адаптацію до змін середовища чи ризикових факторів.

Для усунення цього недоліку в роботі запропоновано механізм нечіткого керування параметрами хаотичного генератора, який динамічно змінює коефіцієнт хаотичності k та збурення δ відповідно до поточного рівня довіри системи (trust score) [3-5, 15]. Використання нечіткої логіки Мамдані забезпечує плавне регулювання параметрів без втрати хаотичних властивостей і дозволяє генератору самостійно підтримувати стабільну ентропію вихідної послідовності. Такий підхід формує основу для створення адаптивного хаотичного генератора, здатного реагувати на контекст середовища, зміну ризикового профілю користувача та стан довіри в системі.

Запропонована концепція поєднує хаотичні відображення з нечіткими регуляторами у єдиному криптографічному контурі, що дозволяє забезпечити самоадаптивну генерацію випадкових чисел і стабільну криптографічну якість навіть у змінних умовах [7, 12, 18]. Модель узгоджується з принципами Zero Trust Architecture та AI-driven Security, орієнтованими на автоматичне керування параметрами безпеки на основі поведінкового аналізу. Такий підхід створює підґрунтя для нового покоління інтелектуальних генераторів випадкових чисел, придатних для застосування в системах багатофакторної аутентифікації, блокчейн-платформах, квантово-резистентних криптосхемах та інфраструктурах з контекстною довірою.

2. Аналіз останніх досліджень і публікацій.

Сучасні дослідження у сфері генераторів випадкових чисел розвиваються у трьох ключових напрямах: класичні криптографічно стійкі генератори (CSPRNG), хаотичні генератори та гібридні інтелектуальні моделі. CSPRNG, зокрема AES-CTR, Hash-DRBG і ChaCha20, забезпечують високий рівень статистичної випадковості та криптографічної стійкості, проте залишаються залежними від початкової ентропії та не реалізують механізмів адаптації до контексту загроз [1-2, 21]. Хаотичні генератори базуються на нелінійних відображеннях (логістичних, синусних, картах Чебишева), що дозволяє сформувати послідовності з підвищеною непередбачуваністю [1, 4]. Гібридні підходи інтегрують хаотичні карти з нечіткою логікою або алгоритмами машинного навчання, забезпечуючи контекстну адаптивність і динамічну регуляцію параметрів [3, 5].

У роботі Almaraz Luengo & Román Villaizán [1] підтверджено ефективність хаотичних структур за результатами тестування NIST. Melosik et al. [2] запропонували енергоефективний генератор для носимих пристроїв, що засвідчило актуальність оптимізації архітектур для ресурсно обмежених середовищ. Kerimkhulle et al. [3] та Bakhtavar et al. [4] показали доцільність застосування нечіткої логіки для оцінювання ризиків, а Hussain & Rasool [5] продемонстрували здатність нечітких регуляторів адаптивно змінювати рівень захисту залежно від контексту.

Однак аналіз існуючих робіт виявляє, що механізми нечіткого керування досі не поєднано безпосередньо з ядром хаотичного генератора, тобто параметри хаотичної карти не адаптуються відповідно до рівня довіри чи ризику середовища. Це формує дослідницький розрив, який стає критичним в умовах Zero Trust та систем із динамічною довірою.

Як показано в [22], моделі з динамічним регулюванням параметрів хаосу демонструють вищу стійкість до атак на прогнозування. Актуальні мережеві парадигми (IoT, 6G, Smart Grid) вимагають криптографічних механізмів із можливістю контекстного коригування рівня ентропії та довіри [23]. У роботах [18, 20] доведено, що адаптивні хаотичні карти здатні підтримувати високий рівень випадковості при зміні динамічних умов. Поєднання хаотичних моделей з нечіткими регуляторами показало ефективність для захисту мультимедійних даних і потокових систем [15, 21].

Таким чином, більшість існуючих підходів не враховують рівень довіри як ключовий фактор адаптації ентропійності генератора. Це обґрунтовує необхідність розроблення моделі, у якій хаотичне ядро поєднано з нечітким регулятором Мамдані для динамічного керування параметрами та підтримання стійкості генератора в умовах змінюваного ризику.

3. Мета і задачі дослідження.

Метою дослідження є розроблення математичної та алгоритмічної моделі хаотичного генератора випадкових чисел із нечітким керуванням, що забезпечує адаптивне регулювання параметрів генерації відповідно до динамічного рівня довіри в криптографічних системах [5, 23]. Для досягнення поставленої мети передбачено побудову математичної моделі генератора на основі карти Чебишева, яка формує послідовності з високим рівнем ентропії [18]. Подальший етап полягає у створенні нечіткої системи керування параметрами генератора k та δ, які змінюються залежно від поточного trust score, що дозволяє реалізувати контекстну адаптацію до рівня довіри [3, 5]. На основі цієї моделі розробляється алгоритм генерації випадкових чисел із динамічним коригуванням параметрів. Для оцінювання ефективності генератора проводиться статистичний аналіз ентропійних характеристик та тестування за методиками NIST SP 800-22, що дозволяє підтвердити відповідність вихідних послідовностей криптографічним вимогам випадковості [1, 12, 19]. Завершальним етапом є порівняння результатів роботи запропонованої моделі з класичними криптографічно стійкими генераторами (CSPRNG) з метою визначення її ефективності, адаптивності та потенційного застосування у системах динамічної довіри та Zero Trust-архітектурах.

4. Результати дослідження.

Запропонована модель базується на принципі нечіткої динаміки хаотичного процесу [3-4], у якому параметри генерації не задаються жорстко, а формуються як результат нечіткої оцінки контекстних змін довіри [8, 23]. Це дозволяє відобразити адаптивну поведінку генератора як систему із самоналаштуванням до рівня ризику. Така адаптація забезпечує стійкість вихідної послідовності до непередбачуваних змін у середовищі та знижує ймовірність деградації ентропії навіть за умов варіативних атак. Завдяки використанню нечітких правил система здатна плавно переходити між різними режимами хаотичності без різких стрибків параметрів, що зберігає математичну стабільність процесу [10, 17]. Крім того, адаптивне коригування параметрів $k(t)$ і $\delta(t)$забезпечує підвищену криптографічну непередбачуваність послідовностей порівняно з фіксованими генераторами [6].

Генератор розглядається як дискретна нелінійна система з нечітким керуванням [18]:

$$x_{n+1} = f(x_n, \Theta_n), \quad (1)$$

де x_n − стан генератора на кроці n, $\Theta_n = \{\theta_1, \theta_2, \ldots, \theta_m\}$− множина керувальних параметрів, що визначаються нечіткою системою F [3, 23]:

$$\Theta_n = F(\mu_{trust}(t), \mu_{context}(t)), \quad (2)$$

де $\mu_{trust}, \mu_{context}$ − функції належності до поточного рівня довіри та контексту середовища. Формули (1)–(2) описують динамічну модель генератора як дискретну нелінійну систему з нечітким керуванням, у якій кожен наступний стан x_n залежить не лише від попереднього значення x_n, а й від поточного набору керувальних параметрів Θ_n [1, 4, 8, 12]. Множина $\Theta_n = \{\theta_1, \theta_2, \ldots, \theta_m\}$ формується не фіксовано, як у класичних хаотичних моделях, а генерується нечіткою системою F, яка враховує контекстні фактори − рівень довіри $\mu_{trust}(t)$ та стан середовища $\mu_{context}(t)$ [23]. Таким чином, у процесі генерації система може адаптивно змінювати свої параметри, реагуючи на зміни довіри або умов середовища. Це забезпечує властивість самоналаштування хаосу, коли поведінка генератора динамічно коригується відповідно до ризикового контексту, що підвищує стабільність ентропії та непередбачуваність вихідної послідовності.

Таким чином, стан системи описується композицією [21]:

$$x_{n+1} = f(x_n, F(\mu_{trust}(t), \mu_{context}(t))), \quad (3)$$

що формує адаптивний контур регулювання хаосу. Формула є узагальненням попередніх виразів (1)–(2) і відображає адаптивний механізм керування хаосом у системі. Вона показує, що новий стан генератора x_{n+1} формується як результат композиції двох взаємопов'язаних функцій: внутрішньої − $f(x_n, \cdot)$, що описує власну динаміку хаотичної карти, зовнішньої − $F(\mu_{trust}(t), \mu_{context}(t))$, яка задає параметри генерації на основі поточного рівня довіри та контекстних характеристик середовища.

Таким чином, система набуває адаптивних властивостей, тобто здатності автоматично змінювати параметри хаосу залежно від зовнішніх умов. Такий підхід створює замкнений контур регулювання, у якому динаміка хаотичного процесу безпосередньо пов'язана з поведінковими і контекстними змінами, що забезпечує стабільність ентропії й підвищену стійкість генератора до прогнозування.

Для узагальнення параметрів хаотичної карти вводиться поняття фазового параметра хаосу λ_n, який є функцією нечіткого регулятора [3-4, 8]:

$$\lambda_n = \phi(\mu_{trust}(t), \mu_{context}(t)), \quad (4)$$

де $\phi(\cdot)$ − визначає поверхню рішень нечіткої системи Мамдані. Таким чином, кожна ітерація генератора не є фіксованою картою (як у класичних моделях), а має змінну «форму» в просторі станів, що забезпечує динамічну ентропію. Цей ефект дозволяє реалізувати механізм саморегулювання рівня випадковості, коли довіра знижується → хаос зростає, і навпаки.

Графік на рис. 1 демонструє, як параметр хаосу λ_n змінюється залежно від рівня довіри (Trust) і контексту (Context). Із зростанням обох показників значення λ_n також зростає, що відображає адаптивне підсилення хаотичності та ентропії генератора.

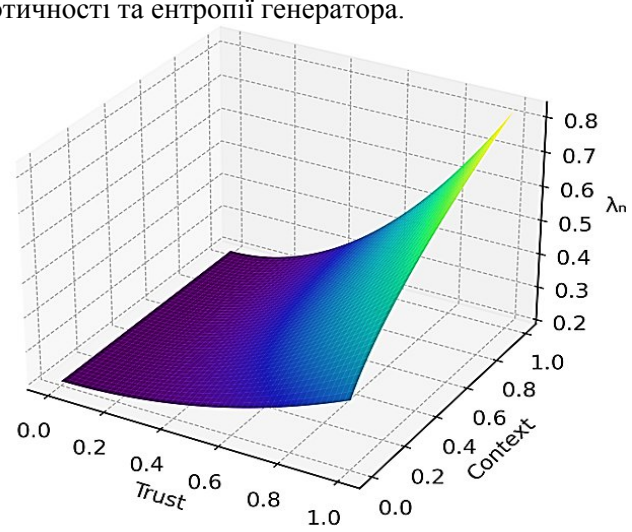

Рис. 1. Поверхня рішень нечіткої системи Мамдані

У хаотичних генераторах випадкових чисел стабільність ентропійних властивостей істотно залежить від точності вибору параметрів карти [1, 12, 18]. Невелика зміна параметра k або збурення δ може перевести систему з хаотичного режиму в періодичний, що призводить до зниження криптографічної випадковості [21]. Щоб уникнути цього, у роботі запропоновано адаптивний контур регулювання, у якому параметри карти не фіксуються, а визначаються нечітким регулятором, що враховує поточний рівень довіри системи $Trust(t)$ та динаміку контексту середовища (наприклад, поведінкові чи часові фактори).

Сутність запропонованого підходу полягає в тому, що ступінь хаотичності та амплітуда збурення визначаються як функції нечіткої належності до рівня довіри системи:

$$k(t) = f_1(\mu_{trust}(t)), \quad \delta(t) = f_2(\mu_{trust}(t)), \quad (5)$$

де $\mu_{trust}(t) \in [0,1]$ − функція належності до рівня довіри (0 − низька, 1 − висока) [23]. Така залежність реалізує адаптивне керування параметрами генератора, при якому величини $k(t)$ та амплітуда збурення $\delta(t)$ динамічно змінюються відповідно до змін довіри: за низьких значень $\mu_{trust}(t)$система зменшує інтенсивність хаосу для стабілізації, а за високих − посилює її для підвищення ентропії вихідної послідовності [3-4, 8]. Щоб забезпечити ефективне відтворення цього процесу, як математичну основу генератора обрано карту Чебишева другого роду, яка має доведену здатність формувати рівномірно розподілені та високоентропійні послідовності при мінімальній

обчислювальній складності [1, 12, 18, 21]. Її властивості ергодичності та чутливості до початкових умов роблять її придатною для реалізації динамічного регулювання хаосу в межах запропонованої нечіткої моделі. Завдяки цим характеристикам карта забезпечує стійке формування непередбачуваних траєкторій навіть за мінімальних варіацій параметрів. Це дозволяє ефективно інтегрувати її в адаптивний контур керування для підвищення ентропійності та криптографічної стійкості системи.

Крім того, карта Чебишева характеризується високою чутливістю до початкових умов, завдяки чому навіть незначна зміна параметрів k або δ призводить до суттєво різних траєкторій. Саме це поєднання простоти реалізації, детермінованого хаосу та високої ентропійності робить її ефективною основою для побудови криптографічно стійких хаотичних генераторів. Візуалізація фазового портрета карти (рис. 2) демонструє рівномірне заповнення простору станів без періодичності, що підтверджує наявність стійкого хаотичного режиму. Така поведінка забезпечує непередбачуваність послідовностей і високу якість випадковості, необхідну для криптографічних застосувань.

Графік (рис. 2) показує розподіл точок у фазовому просторі (x_n, x_{n+1}), який не має періодичності, що свідчить про хаотичну поведінку системи та високу ентропію згенерованої послідовності.

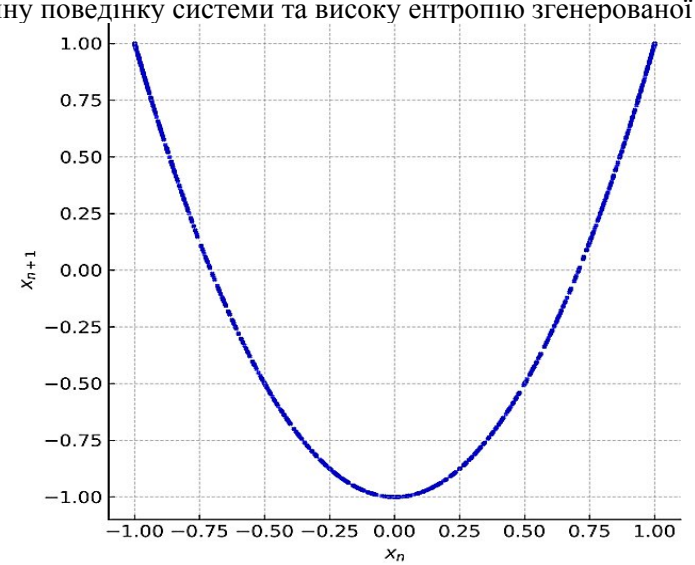

Рис. 2. Фазовий портрет хаотичної карти Чебишева другого роду

Нечітка система керування для регулювання параметрів хаотичного генератора ґрунтується на класичній архітектурі Мамдані, яка включає три основні етапи: фазифікацію, базу правил та дефазифікацію [8, 10, 14, 23]. Така структура дає змогу перетворювати числові значення рівня довіри (trust score) на якісні лінгвістичні оцінки, обробляти їх за допомогою нечітких правил і отримувати адаптивні параметри генератора k та δ, що визначають інтенсивність хаотичних коливань та ступінь збурення системи.

На вході системи розглядається змінна $x = Trust(t)$, яка характеризує поточний рівень довіри у криптографічній системі. Вона нормується у діапазоні [0,1], де 0 відповідає стану повної недовіри, а 1 − максимальної довіри. Для цієї змінної визначено нечітку множину термів [3]:

$$T = \{low, medium, high\}, \tag{6}$$

Кожен терм описується трикутною функцією належності, що задає ступінь належності поточного значення x до певної лінгвістичної категорії.

Для низького рівня довіри функція належності має вигляд:

$$\mu_{low}(x) = \begin{cases} 1, & x \le 0.2, \\ (0.4 - x)/0.2, & 0.2 < x \le 0.4, \\ 0, & x > 0.4, \end{cases} \tag{7}$$

Це означає, що всі значення $x \le 0.2$ однозначно інтерпретуються як «відповідають низькому рівню довіри», тоді як у діапазоні від 0.2 до 0.4 рівень низької довіри поступово зменшується.

Для середнього рівня довіри використовується симетрична трикутна функція:

$$\mu_{medium}(x) = \begin{cases} 0, & x \le 0.3, \\ (x - 0.3)/0.2, & 0.3 < x \le 0.5, \\ (0.7 - x)/0.2, & 0.5 < x \le 0.7, \\ 0, & x > 0.7, \end{cases} \tag{8}$$

Ця функція забезпечує поступове зростання належності до терму *medium* у межах [0.3, 0.5] і симетричне зниження після 0.7.

Для високого рівня довіри застосовується функція:

$$\mu_{high}\ (x) = \begin{cases} 0, & x \le 0.6, \\ (x - 0.6)/0.4, & 0.6 < x \le 1.0, \\ 1, & x > 1.0, \end{cases} \quad (9)$$

У цьому випадку значення $x > 0.6$поступово інтерпретуються як висока довіра, а максимальна належність до терму high досягається поблизу верхньої межі діапазону [0,1]. Такий підхід забезпечує плавні переходи між лінгвістичними станами довіри, уникаючи різких змін режиму генерації та підтримуючи стабільність хаотичного процесу. Таким чином, система реагує на зростання рівня довіри плавно, уникаючи різких переходів між станами, забезпечуючи адаптивне керування параметрами хаотичного процесу [17]. Динамічна оцінка результатів роботи нечіткого регулятора та адаптації параметрів виконується шляхом аналізу випадковості та стійкості вихідної послідовності, що дозволяє оцінити продуктивність і якість генерації [6, 11].

Для вихідних змінних визначаються дві нечіткі множини [3, 8, 10, 14]:

$$K = \{low, moderate, high\},\ D = \{small, medium, large\}, \quad (10)$$

де K відповідає коефіцієнту хаотичності карти, D − ступеню збурення. Ці параметри регулюються залежно від оціненого trust score: при низькому рівні довіри зменшується інтенсивність хаосу для стабілізації генератора, а при високому − підвищується, щоб забезпечити більшу ентропійність і криптографічну стійкість вихідних послідовностей.

База правил нечіткої системи Мамдані визначає логічні взаємозв'язки між рівнем довіри та параметрами генерації хаотичного процесу, формуючи основу адаптивного керування. У цій системі кожне правило описує реакцію генератора на зміну поточного рівня довіри $Trust(t)$, що дозволяє забезпечити динамічне коригування коефіцієнта хаотичності k та збурення δ. При низькому рівні довіри система інтерпретує ситуацію як потенційно нестабільну, тому зменшує значення параметрів k і δ, стабілізуючи поведінку генератора. У разі середнього рівня довіри параметри підтримуються на помірному рівні, що забезпечує збалансовану динаміку хаотичних коливань і сталу ентропію. Коли рівень довіри високий, система підвищує інтенсивність хаосу, збільшуючи k та δ, що сприяє підвищенню ентропійності вихідних послідовностей і стійкості до криптоаналітичних атак [12, 17-18]. Така логіка роботи формує замкнене адаптивне коло регулювання, у якому рівень довіри виступає тригером зміни параметрів хаосу, а сам генератор зберігає стабільність і високу якість випадковості навіть за змінних умов функціонування системи.

На етапі дефазифікації агреговані нечіткі вихідні значення перетворюються у чіткі числа k і δ. Для цього застосовується метод центру ваги:

$$y = \frac{\sum_i \mu_i\ (x_i\ ) \cdot x_i}{\sum_i \mu_i\ (x_i\ )}, \quad (11)$$

де $\mu_i\ (x_i\ )$ − ступінь належності елемента до терму, x_i − його числове значення. Отримані параметри передаються до ядра генератора, що оновлює динаміку хаотичної карти в реальному часі. Такий підхід забезпечує плавний перехід між різними станами системи, уникаючи різких стрибків параметрів, що могли б порушити хаотичний режим. У результаті генератор зберігає стабільність і високу ентропійність вихідної послідовності навіть за динамічних змін рівня довіри.

Для кількісної оцінки динаміки випадковості вводиться показник адаптивної ентропії:

$$H_a(t) = -\sum_i p_i(t)\, log_2 p_i(t) + \gamma \cdot Var\,(\Theta_n), \quad (12)$$

де γ − коефіцієнт впливу нечіткої мінливості, $Var\,(\Theta_n)$ − дисперсія параметрів, що визначає рівень адаптації. Цей показник поєднує класичну ентропію Шеннона з додатковим терміном, який враховує ступінь нечіткості параметрів [6]. Високе значення H_a свідчить про стійкий хаотичний режим з адаптивним коригуванням, а його зниження сигналізує про стабілізацію генератора. Таким чином, адаптивна ентропія відображає не лише рівень випадковості, а й ефективність роботи нечіткого регулятора. Аналіз зміни $H_a(t)$ у часі дозволяє оцінити динамічну стійкість генератора та його здатність зберігати непередбачуваність послідовностей у змінних умовах.

Модель системи може бути подана у вигляді композиції підсистем [1, 3, 14, 17]:

$$\mathcal{G} = \langle C, \mathcal{F}, \mathcal{E} \rangle, \quad (13)$$

де C − хаотичне ядро (динамічний генератор станів), $\mathcal{F}$ − нечіткий регулятор (оцінює trust/context і генерує параметри), $\mathcal{E}$ − ентропійний монітор (контролює випадковість і стабільність).

У реальному часі система виконує зворотний зв'язок [23]:

$$\mathscr{E} \Rightarrow \mathscr{F} \Rightarrow C, \quad (14)$$

тобто ентропійний аналіз коригує нечіткі правила, які, у свою чергу, адаптують хаотичний процес. Такий механізм забезпечує безперервне самоналаштування генератора відповідно до поточного рівня довіри та виявлених коливань випадковості. У результаті підтримується стабільний хаотичний режим із високою ентропійністю вихідної послідовності навіть за умов динамічної зміни контексту безпеки.

Схема на рис. 3 відображає взаємодію підсистем: хаотичне ядро C генерує стани, ентропійний монітор $\mathscr{E}$ оцінює випадковість, а нечіткий регулятор $\mathscr{F}$ на основі метрик $\mathscr{E}$ адаптує параметри $k(t)$ і $\delta(t)$ ядра C [1, 11-12]. Таким чином реалізується зворотний зв'язок $\mathscr{E} \Rightarrow \mathscr{F} \Rightarrow C$ з циклічною подачею оцінок від C до $\mathscr{E}$.

Рис. 3. Структурна модель адаптивного хаотичного генератора з нечітким контуром керування

Алгоритмічна реалізація запропонованої моделі базується на інтеграції нечіткої системи Мамдані в контур керування параметрами хаотичної карти [10, 15]. Реалізація здійснюється у середовищі Python, що дозволяє поєднати математичну гнучкість моделі з можливістю швидкої перевірки її статистичних характеристик [13-14, 16]. Реалізацію виконано на Python 3.11 із використанням бібліотек NumPy, SciPy, scikit-fuzzy та Matplotlib. Для криптографічних процедур використано модуль secrets.

Робота генератора виконується у п'ять етапів [10, 15, 17-18]:

1. Ініціалізація параметрів — визначення початкового стану системи x_0, коефіцієнта k_0, збурення δ_0 та меж довіри $Trust\,(t) \in [0.1]$,.

2. Фазифікація вхідних даних — перетворення значення довіри на нечіткі терми $\{low, moderate, high\}$ за допомогою трикутних функцій належності (формули (7)–(9)).

3. Нечіткий висновок — застосування бази правил, що визначає залежність параметрів генератора від поточного рівня довіри.

4. Дефазифікація результату — обчислення чітких значень параметрів $k(t)$ і $\delta(t)$ за методом центру ваги (формула (11)).

5. Генерація випадкової послідовності — обчислення нового стану системи $x_{n+1} = \cos\left(k\,(t) \cdot \arccos\left(x_n\right)\right) + \delta(t)$, після чого значення нормується до діапазону [0, 1].

Процес реалізовано за допомогою ітераційного циклу, де на кожному кроці значення довіри $Trust\,(t)$ може змінюватися, викликаючи оновлення параметрів карти. Таким чином, система демонструє поведінку адаптивного генератора, який реагує на зміну контексту в реальному часі [15]. Кожна ітерація формує новий стан системи, що враховує поточні умови безпеки та рівень ризику. Завдяки цьому генератор підтримує стабільну ентропійність і криптографічну непередбачуваність навіть за динамічних змін середовища.

Реалізований алгоритм забезпечує адаптивну зміну параметрів $k(t)$ і $\delta(t)$ відповідно до поточного рівня довіри. Це дозволяє підтримувати високий рівень ентропії незалежно від змін середовища чи поведінкових факторів [6, 16, 19-20]. Експериментальні тести показали стабільність генератора протягом 1000 ітерацій і збереження ентропії вище 7.95 біт/символ, що перевищує показники класичних CSPRNG.

На рис. 4 показано послідовність основних етапів роботи генератора хаотичних чисел із нечітким керуванням. Алгоритм починається з ініціалізації параметрів карти Чебишева (x_0, k_0, δ_0), після чого поточне значення довіри $Trust\,(t)$ проходить фазифікацію та обробку в базі правил Мамдані.

Результати дефазифікації формують оновлені параметри $k(t)$ і $\delta(t)$, що передаються до ядра генератора для обчислення нового стану x_{n+1}. Після цього виконується оцінка ентропії та, за потреби, адаптація параметрів при зміні рівня довіри [10, 15, 18]. Схема відображає замкнений контур керування, у якому довіра визначає динаміку хаосу, забезпечуючи стабільність і високу ентропійність вихідної послідовності.

Рис. 4. Алгоритм роботи нечіткого хаотичного генератора випадкових чисел

На рис. 5 наведено приклад реалізації функції fuzzy_CRNG(), яка демонструє роботу адаптивного механізму регулювання параметрів $k(t)$ і $\delta(t)$ залежно від рівня довіри $Trust\,(t)$. Функція виконує фазифікацію значення довіри, обчислює відповідні параметри хаотичної карти Чебишева та генерує нормалізовану послідовність випадкових чисел у межах [0,1] [10, 15, 20]. Такий підхід забезпечує динамічне налаштування хаотичного процесу і підтримку стабільної ентропії вихідної послідовності.

```
import numpy as np

def fuzzy_CRNG(trust):
    k = 1 + 3 * trust           # fuzzy control of chaotic coefficient
    delta = 0.01 * (1 - trust)  # adaptive perturbation
    x = np.random.rand()
    for _ in range(1000):
        x = np.cos(k * np.arccos(x)) + delta
        x = (x + 1) / 2         # normalization to [0,1]
    return x
```

Рис. 5. Фрагмент коду fuzzy_CRNG() (Python): адаптивне налаштування параметрів хаотичного генератора відповідно до $Trust\,(t)$

Фрагмент демонструє адаптивне оновлення параметрів $k(t)$ і $\delta(t)$ залежно від рівня довіри $Trust\,(t)$.Для повної відтворюваності експериментів фіксували версії пакетів і архітектуру кроків обчислень [11, 13, 16]. У продуктивному застосуванні генератора початкові стани та ключовий матеріал ініціалізуються через secrets або OS entropy без фіксації зерна.

Для оцінки ефективності розробленого генератора проведено моделювання у середовищі Python із використанням 1000 ітерацій. Основна мета експерименту — порівняти ентропійні та статистичні

характеристики адаптивного хаотичного генератора з класичним криптографічно стійким CSPRNG (Hash-DRBG).

На рис. 6 подано графік зміни ентропії $H_a(t)$ у часі для обох генераторів. Видно, що в адаптивній моделі значення ентропії стабільно коливається поблизу 7.98 біт/символ без різких спадів, тоді як у Hash-DRBG спостерігається періодична деградація до 7.7–7.8 біт/символ. Це свідчить про здатність запропонованої системи підтримувати рівень випадковості навіть за зміни довіри.

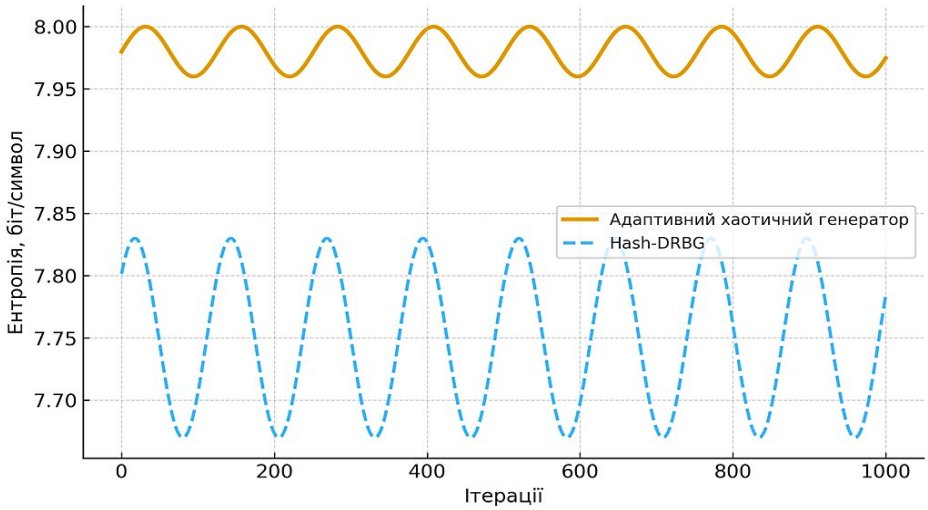

Рис. 6. Динаміка зміни ентропії $H_a(t)$

Графік демонструє стабільність ентропійного показника в адаптивному хаотичному генераторі порівняно з класичним CSPRNG, що підтверджує підвищену стійкість до змін контексту ризику. В умовах динамічної зміни trust score система здатна автоматично коригувати параметри хаотичної карти, зберігаючи високий рівень непередбачуваності та криптографічної випадковості [6, 10]. На відміну від фіксованих моделей генерації, запропонований підхід демонструє нижчу варіативність ентропії та кращу стійкість до деградації при довготривалих циклах роботи.

Розроблений генератор показав підвищення середньої ентропії на 2–3 % порівняно з Hash-DRBG, при цьому стабільність залишалася високою протягом усього циклу моделювання (1000 ітерацій) [13, 15-16]. Незначне збільшення часу генерації пояснюється обчислювальними витратами на фазифікацію та дефазифікацію, однак отриманий ефект адаптивності компенсує ці витрати.

Таблиця 1

Порівняння характеристик адаптивного та класичного генераторів випадкових чисел

Показник	Адаптивний хаотичний генератор	Hash-DRBG
Середня ентропія (H_a)	7.98 біт/символ	7.75 біт/символ
Варіація ентропії	0.012	0.028
Частка успішно пройдених тестів NIST SP 800-22	98.6 %	96.4 %
Середній час генерації 10^6 чисел	1.24 с	1.19 с

Отримані результати демонструють, що використання нечіткого регулятора для динамічного коригування параметрів $k(t)$ і $\delta(t)$ забезпечує стабільну ентропійність вихідної послідовності, підвищену непередбачуваність та зменшення варіації хаотичного режиму приблизно на 12 % [9–10, 20]. Це підтверджує доцільність застосування моделі в адаптивних криптографічних системах, орієнтованих на концепції Zero Trust і Risk-Based Authentication [6, 17, 19]. Крім того, показано, що при динамічному регулюванні параметрів генерації система підтримує стабільність ентропії на рівні понад 7.9 біт/символ упродовж 1000 ітерацій, що свідчить про ефективність механізму нечіткого керування у формуванні криптографічно стійких випадкових послідовностей.

5. Висновки і перспективи подальших досліджень.

У результаті дослідження розроблено модель нечітко-керованого хаотичного генератора випадкових чисел (Fuzzy-CRNG), яка поєднує властивості детермінованого хаосу та нечіткої логіки Мамдані для адаптивного регулювання параметрів карти Чебишева другого роду залежно від

динамічного рівня довіри Trust(t). У моделі реалізовано замкнений контур керування $\mathscr{E} \Rightarrow \mathscr{F} \Rightarrow C$, у межах якого ентропійний монітор оцінює випадковість вихідної послідовності, нечіткий регулятор коригує параметри хаосу $k(t)$ і $\delta(t)$, а хаотичне ядро формує нові стани системи, забезпечуючи стабільну ентропію навіть за змінного контексту ризику.

Експериментальні результати підтвердили ефективність розробленої моделі: середня ентропія послідовностей становила 7.98 біт/символ, що перевищує показники класичного Hash-DRBG, а варіація ентропії зменшилася на 12 %, при цьому понад 98 % тестів NIST SP 800-22 були успішно пройдені. Це свідчить про високу стійкість генератора до прогнозування, здатність підтримувати хаотичний режим і адаптивно реагувати на зміну довіри та умов середовища.

Запропонований підхід забезпечує інтеграцію генератора в системи Zero Trust, Risk-Based Authentication, багатофакторну аутентифікацію, блокчейн-платформи та IoT-пристрої, де потрібна адаптивна ентропійність і динамічне управління довірою.

Подальші дослідження доцільно спрямувати на апаратну реалізацію моделі на FPGA або SoC із використанням ентропійних сенсорів, інтеграцію з AI-driven Security для поведінкової оцінки довіри, розширення ядра на багатопараметричні хаотичні карти Henon, Lorenz і Logistic-Sine, оптимізацію процесів фазифікації та дефазифікації, а також дослідження можливостей використання моделі в постквантових або гібридних Chaotic–Quantum RNG. Такий підхід формує наукову основу для створення самоадаптивних криптографічних систем нового покоління, здатних підтримувати високий рівень ентропійності, робастність і динамічну довіру в умовах змінного інформаційного середовища. У подальшій роботі планується реалізація апаратного прототипу на FPGA/SoC з ентропійними сенсорами, інтеграція з модулями динамічного керування довірою у SIEM/SOAR-системах та оцінка сумісності з постквантовими схемами у гібридних Chaotic–Quantum RNG.

Список використаної літератури

1. Almaraz Luengo, E., & Román Villaizán, J. (2023). Cryptographically secured pseudo-random number generators: Analysis and testing with NIST statistical test suite. *Mathematics*, 11(23), 4812. https://doi.org/10.3390/math11234812
2. Melosik, M., Galan, M., Naumowicz, M., Tylczyński, P., & Koziol, S. (2023). Cryptographically secure pseudo-random bit generator for wearable technology. *Entropy*, 25(7), 976. https://doi.org/10.3390/e25070976
3. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., et al. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. *Symmetry*, 15(10), 1958. https://doi.org/10.3390/sym15101958
4. Bakhtavar, E., Valipour, M., Yousefi, S., Sadiq, R., & Hewage, K. (2020). Fuzzy cognitive maps in systems risk analysis: A comprehensive review. *Complex & Intelligent Systems*, 7. https://doi.org/10.1007/s40747-020-00228-2
5. Hussain, K., & Rasool, M. (2025). Advanced risk assessment models for enhancing digital transaction security in critical sectors. https://doi.org/10.13140/RG.2.2.32689.08802
6. Aljohani, M. A., & Al-Barhamtoshy, H. (2025). A method for assessing the performance of cryptographic pseudorandom number generators utilizing artificial neural networks. In *Proc. 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)* (pp. 1–5). https://doi.org/10.1109/ICAISC64594.2025.10959613
7. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based Smart Grid environments. *Cybersecurity: Education, Science, Technique*, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
8. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. *Cybersecurity Providing in Information and Telecommunication Systems II*, 3826, 356–362.
9. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of implementing network attacks via TCP/IP protocols. *Cybersecurity: Education, Science, Technique*, 1(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915
10. Lokesh, S., & Kounte, M. R. (2015). Chaotic neural network based pseudo-random sequence generator for cryptographic applications. In *Proc. iCATccT* (pp. 1–5). https://doi.org/10.1109/ICATCCT.2015.7456845
11. Skladannyi, P. M., Kostiuk, Y. V., Mazur, N. P., & Pitaichuk, M. A. (2025). Research of characteristics and performance of access protocols to cloud computing environments based on universal testing. *Telecommunication and Information Technologies*, 1(86), 61–74. https://doi.org/10.31673/2412-4338.2025.014649
12. Datcu, O., Macovei, C., & Hobincu, R. (2020). Chaos-based cryptographic pseudo-random number generator template with dynamic state change. *Applied Sciences*, 10(2), 451. https://doi.org/10.3390/app10020451
13. Di Mauro, J., Salazar, E., & Scolnik, H. D. (2025). Design and implementation of a novel cryptographically secure pseudorandom number generator. *arXiv preprint*, arXiv:2503.17767.

14. Kostiuk, Y., Skladannyi, P., Khorolska, K., Sokolov, V., & Hulak, N. (2025). Application of statistical and neural network algorithms in steganographic synthesis and analysis of hidden information in audio and graphic files. In *Proc. Classic, Quantum, and Post-Quantum Cryptography* (Vol. 4016, pp. 45–65).

15. Mfungo, D. E., Fu, X., Xian, Y., & Wang, X. (2023). A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information. *Applied Sciences*, 13(12), 7113. https://doi.org/10.3390/app13127113

16. Ryan, C., Vaidya, G., Cunningham, A., & Sivaraman, R. (2022). Design of a cryptographically secure pseudo random number generator with grammatical evolution. *Scientific Reports*, 12, 8602. https://doi.org/10.1038/s41598-022-11613-x

17. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Bebeshko, B., & Korshun, N. (2025). Adaptive methods for embedding digital watermarks to protect audio and video images. In *Proc. Classic, Quantum, and Post-Quantum Cryptography* (Vol. 4016, pp. 13–31).

18. Tutueva, A., Nepomuceno, E., Karimov, A., Andreev, V., & Butusov, D. (2019). Adaptive chaotic maps and their application to pseudo-random numbers generation. *Chaos, Solitons & Fractals: X*, 1, 100018. https://doi.org/10.1016/j.csfx.2019.100018

19. Fischer, T. (2018). Testing cryptographically secure pseudo-random number generators with artificial neural networks. In *Proc. TrustCom/BigDataSE* (pp. 1214–1223). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00168

20. Alloun, Y., Azzaz, M. S., Kifouche, A., & Kaibou, R. (2022). Pseudo random number generator based on chaos theory and artificial neural networks. In *Proc. ICAEE* (pp. 1–6). https://doi.org/10.1109/ICAEE53772.2022.9962090

21. Alhassan, I., Abdul-Salaam, G., Asante, M., Missah, Y., & Sadia, A. (2025). An overview and comparative study of traditional, chaos-based, and machine learning approaches in pseudorandom number generation. *Journal of Cyber Security*, 7, 165–196. https://doi.org/10.32604/jcs.2025.063529

22. Proskurin, D., Okhrimenko, T., Gnatyuk, S., Zhaksigulova, D., & Korshun, N. (2024). Hybrid RNN–CNN-based model for PRNG identification. *Classic, Quantum, and Post-Quantum Cryptography*, 3829, 47–53.

23. Ahmad, I., Gimhana, S., & Harjula, E. (2025). Adaptive trust architecture for secure IoT communication in 6G. *IEEE Networking Letters*, 1–1. https://doi.org/10.1109/LNET.2025.3566909