ВІСНИК ПРИАЗОВСЬКОГО ДЕРЖАВНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
2026р. Серія: Технічні науки Вип. 53. Т. 1
p-ISSN: 2225-6733; e-ISSN: 2519-271X

УДК 004.9 DOI: 10.31498/2225-6733.53.1.2026.359779

ІМІТАЦІЙНА МОДЕЛЬ ЕЛЕКТРОННОГО НЕЛІНІЙНОГО ОСЦИЛЯТОРА ДЛЯ ГЕНЕРАЦІЇ ВИСОКОЕНТРОПІЙНИХ ПОСЛІДОВНОСТЕЙ У ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ

Левицька Т.О. *канд. техн. наук, доцент, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, ORCID: https://orcid.org/0000-0003-3359-1313, e-mail: levitskaya_t_a@pstu.edu;*

Носовська С.Є. *ст. викладач, ДВНЗ «Приазовський державний технічний університет», м. Дніпро, ORCID: https://orcid.org/0000-0002-6176-6101, e-mail: nosovska_s_e@pstu.edu*

Сучасні системи захисту інформації та захищені канали зв'язку потребують джерел високої ентропії та стійкості до передбачуваності. У статті запропоновано підхід до моделювання та програмної реалізації електронного нелінійного осцилятора як джерела псевдовипадкових послідовностей для криптографічних застосувань. В якості математичного апарату обрано модель осцилятора Чуа, що дозволяє досліджувати динаміку нелінійних систем третього порядку та вивчати умови виникнення детермінованого хаосу. Модифікована система рівнянь включає додатковий коефіцієнт керування, що розширює область існування хаотичних атракторів та забезпечує гнучке управління режимами коливань. Чисельне моделювання динаміки системи виконано методом Рунге–Кутти четвертого порядку, що забезпечує високу точність відтворення траєкторій і стабільність хаотичного режиму за умови експоненціальної чутливості системи до початкових умов. Для програмної реалізації застосовано об'єктно-орієнтований підхід, що дозволив структурувати комплекс як сукупність взаємодіючих об'єктів, включаючи генератор хаосу та модуль криптографічної обробки даних. Використання UML-діаграм класів і послідовностей забезпечує модульність, масштабованість і зрозумілу взаємодію компонентів системи. Особлива увага приділена методам формування хаотичної гами та її застосуванню для криптографічного маскування інформаційного сигналу, що гарантує непередбачуваність вихідних послідовностей. Проаналізовано динамічні режими системи, побудовано матрицю «параметр–режим» та визначено вплив початкових умов і параметрів на стабільність хаотичного режиму, що важливо для забезпечення надійності криптографічного захисту. Таким чином, дослідження поєднує математичне моделювання, чисельні методи та об'єктно-орієнтовану архітектуру програмного комплексу для створення надійного джерела високоефективних псевдовипадкових послідовностей, придатних для сучасних криптографічних застосувань та захисту інформаційних потоків.

Ключові слова: *захист інформації; імітаційне моделювання; нелінійний осцилятор; детермінований хаос; псевдовипадкові послідовності; метод Рунге–Кутти; UML-проєктування; криптографічна стійкість.*

Постановка проблеми

На сучасному етапі розвитку інформаційних технологій безпека передачі та зберігання даних є одним із ключових пріоритетів. Ефективність більшості криптографічних протоколів безпосередньо залежить від якості генераторів псевдовипадкових чисел (ГПЧ), що застосовуються для формування ключів шифрування, ініціалізуючих векторів і автентифікаційних параметрів.

Традиційні алгоритмічні ГПЧ, засновані на лінійних конгруентних методах або регістрах зсуву, характеризуються обмеженою періодичністю та потенційною передбачуваністю. За наявності достатнього обсягу вихідних даних можливе відновлення внутрішнього стану генератора, що створює критичні вразливості для систем захисту інформації в умовах зростання обчислювальних потужностей.

Використання фізичних джерел ентропії здатне підвищити криптографічну стійкість, однак їх інтеграція у цифрові системи пов'язана з технічною складністю та підвищеною вартістю. У зв'язку з цим актуальним науково-технічним завданням є розробка імітаційних моделей нелінійних динамічних систем, що демонструють режим детермінованого хаосу. Такі системи поєднують алгоритмічну відтворюваність за фіксованих початкових умов із властивостями природного хаосу – неперіодичністю, високою ентропією та експоненціальною чутливістю до початкових параметрів.

Процес перенесення неперервної хаотичної динаміки у дискретне програмне середовище потребує комплексного розв'язання низки науково-практичних задач. Насамперед це стосується забезпечення математичної точності шляхом обґрунтованого вибору чисельних методів, здатних мінімізувати похибки округлення та зберегти інваріантні властивості атрактора на великих інтервалах інтегрування. Водночас особлива увага приділяється формуванню програмної архітектури на засадах масштабованих об'єктно-орієнтованих моделей, що дозволяє адаптувати систему до використання в середовищах із різними обчислювальними ресурсами. Ключовим аспектом при цьому виступає статистична надійність, яка гарантує повну відповідність генерованих бітових послідовностей суворим сучасним критеріям випадковості, що висуваються до криптографічних застосувань.

Отже, розробка та дослідження імітаційної моделі електронного нелінійного осцилятора як програмного компонента систем захисту інформації є актуальним напрямом підвищення криптографічної стійкості в сучасних інформаційно-комунікаційних системах.

Copyright © 2026, Authors. This is an open access article under the Creative Commons CC BY license

Аналіз останніх досліджень та публікацій

У сучасній науковій літературі останніх років спостерігається чітка тенденція інтеграції нелінійних динамічних систем у криптографічні застосування [1, 2]. Багатовимірні хаотичні системи з прихованими атракторами та їх апаратна реалізація дозволяють значно підвищити надійність криптосистем [3, 4]. Фундаментальні аспекти генерації псевдовипадкових чисел, включно з критеріями якості та порівняльними оглядами методів, детально висвітлено в оглядових роботах [5, 6].

Деякі дослідження пропонують застосування гамільтонових консервативних систем [7] або вдосконалених логістичних мап [8]. Особливу увагу привертають підходи, що поєднують хаотичні карти з квантовими випадковими ходами [9, 10], а також фізичні квантові генератори (QRNG) [11].

Практична ефективність просторових і гіперхаотичних моделей підтверджується їх застосуванням у шифруванні зображень через глобальні бітові перестановки [12, 13] та гібридне керування цифровими картами [14, 15]. Часто такі генератори реалізуються на мікроконтролерах та вбудованих системах [16]. Новітні підходи також включають алгоритм Гартлі [17] і методи машинного навчання, наприклад, нейромережі WGAN-GP, для синтезу статистично стійких послідовностей [18].

Попри значну кількість робіт, питання універсального програмно-орієнтованого моделювання генераторів псевдовипадкових чисел залишається відкритим. Більшість досліджень зосереджені на цифрових імплементаціях та математичному аналізі їхньої динаміки [19], тоді як об'єктно-орієнтоване моделювання і точність переходу від неперервної до дискретної моделі потребують додаткового вивчення [20].

Мета статті

Метою цієї статті є розробка та дослідження об'єктно-орієнтованої імітаційної моделі електронного нелінійного осцилятора, який може використовуватися як програмний компонент для генерації криптографічно стійких псевдовипадкових послідовностей. Для досягнення цієї мети необхідно сформулювати математичний опис динамічної системи, здатної функціонувати в режимі детермінованого хаосу, а також обґрунтувати вибір чисельних методів інтегрування, що забезпечують збереження ключових властивостей атрактора при переході до дискретного середовища. Додатково передбачено побудову програмної архітектури генератора на принципах об'єктно-орієнтованого підходу з урахуванням вимог масштабованості та можливості інтеграції в сучасні інформаційно-комунікаційні системи.

Матеріали та методи

Об'єктом дослідження є програмний прототип генератора псевдовипадкових чисел на основі електронного нелінійного осцилятора. Він використовує математичну модель тривимірної хаотичної системи з прихованим атрактором, чисельне інтегрування методом Рунге-Кутти четвертого порядку для побудови фазових траєкторій та алгоритм побітової екстракції ентропії з молодших розрядів координат.

Для аналізу поведінки системи застосовано методи теорії детермінованого хаосу, зокрема вивчення точок біфуркації та обчислення показників Ляпунова. Принципи об'єктно-орієнтованого проектування (UML) використано для побудови архітектури моделі, а статистична оцінка за стандартом NIST SP 800-22 дозволяє перевірити криптографічну стійкість згенерованих послідовностей.

На основі аналізу сучасних підходів [1, 8] побудовано модель перетворення неперервної динаміки осцилятора у дискретний потік даних. Визначено критерії вибору кроку інтегрування для мінімізації деградації хаосу та реалізовано демонстраційний приклад програмного комплексу, який забезпечує лавинний ефект при зміні початкових умов і параметрів системи.

Виклад основного матеріалу

Складність структурної організації хаотичних сигналів, їхня виражена нерегулярність, а також експоненціальна чутливість до мінімальних відхилень початкових умов відкривають широкі перспективи для використання детермінованого хаосу в сучасній криптографії. Саме ці властивості дозволяють одному й тому ж алгоритму генерувати некорельовані процеси, що є фундаментом для створення криптографічно стійких систем захисту інформації.

У даному дослідженні як базовий математичний апарат обрано модель осцилятора Чуа. Вибір зумовлений тим, що при відносній простоті опису (система складається лише з трьох диференціальних рівнянь), вона демонструє надзвичайно складну нелінійну динаміку, притаманну стохастичним процесам. Це робить її найбільш ефективною з точки зору програмної та апаратної реалізації в системах шифрування.

Математичний опис динаміки системи у безрозмірній формі, яка є найбільш зручною для імітаційного моделювання, представляється системою автономних диференціальних рівнянь:

$$\begin{cases} C_1 \frac{dv_{C_1}}{dt} = G\left(v_{C_2} - v_{C_1}\right) - g\left(v_{C_1}\right) \\ C_2 \frac{dv_{C_2}}{dt} = G\left(v_{C_1} - v_{C_2}\right) - i_L \\ L \frac{di_L}{dt} = -v_{C_2} \end{cases} \quad (1)$$

p-ISSN: 2225-6733; e-ISSN: 2519-271X

де f(x) – кусково-лінійна функція, що описує нелінійну характеристику системи та визначається наступним математичним виразом:

$$g(v_{C_1}) = G_b v_{C_1} + \frac{1}{2}(G_a - G_b)(|v_{C_1} + E| - |v_{C_1} - E|) \quad (2)$$

Графічне представлення нелінійної функції (2) наведено на рис. 1, де параметри G_a та G_b визначають крутизну внутрішньої та зовнішньої ділянок відповідно; при цьому точки перегину (зламу) на графіку позначені як E.

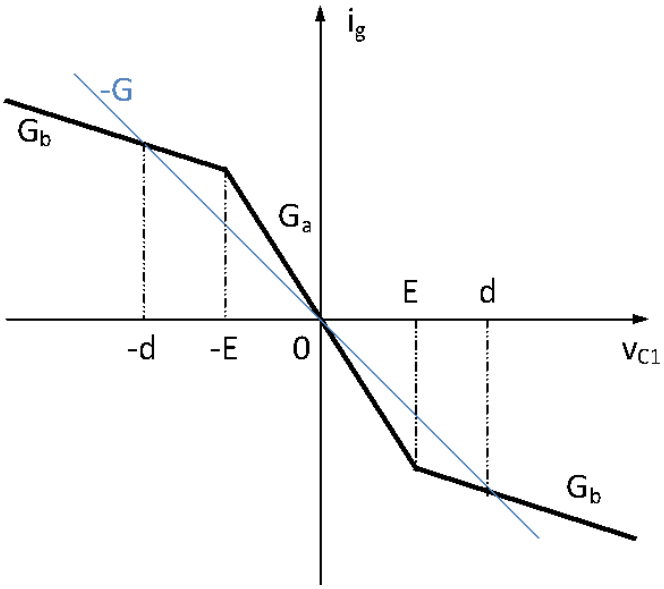

Рис. 1 – Графік вольт-амперної характеристики діода Чуа

На графіку також відображено навантажувальну пряму, в точках перетину якої з вольт-амперною характеристикою формуються три стани рівноваги: d, 0 та -d.

Шляхом переходу до безрозмірних коефіцієнтів у системі диференціальних рівнянь (1), математична модель набуває вигляду, найбільш зручного для програмної реалізації та імітаційного моделювання:

$$\begin{cases} \frac{dx}{dt} = a(y - x - h(x)) \\ \frac{dy}{dt} = x - y + z \\ \frac{dz}{dt} = -\beta y \end{cases} \quad (3)$$

де функція f(x) визначена як:

$$h(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x + 1| - |x - 1|) \quad (4)$$

У межах даної роботи було застосовано модифіковану математичну модель, в яку введено додатковий коефіцієнт c. Це дозволяє забезпечити гнучкіше керування режимами коливань системи та розширити область існування хаотичних атракторів. Модифікована система рівнянь має наступний вигляд:

$$\begin{cases} \frac{dx}{dt} = a(y - x - h(x)) \\ \frac{dy}{dt} = c(x - y + z) \\ \frac{dz}{dt} = -\beta y \end{cases} \quad (5)$$

Математична структура функції h(x) у модифікованій системі рівнянь (5) залишається ідентичною її аналітичному визначенню, наведеному у формулі (4). Це забезпечує збереження ключових властивостей нелінійності, необхідних для генерації хаотичних процесів, навіть при введенні додаткового коефіцієнта керування c. Результати чисельного моделювання отриманої системи рівнянь підтверджують, що за умови дотримання специфічних співвідношень між параметрами моделі, динаміка змінних набуває вираженого хаотичного характеру. Слід зауважити, що стійкі режими хаотичних коливань локалізовані у відносно вузьких діапазонах значень параметрів, що висуває високі вимоги до точності обчислювальних алгоритмів та вибору початкових умов.

Аналіз динамічних режимів системи показав, що за певних значень параметрів в околі точок рівноваги d або -d виникає стійкий граничний цикл. У разі подальшої зміни керуючих коефіцієнтів у системі спостерігається каскад подвоєння періоду, що є класичним шляхом переходу до детермінованого хаосу, зокрема до формування атрактора типу Ресслера.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

При досягненні критичних значень параметрів, що відповідають режиму розвиненого хаосу, відбувається об'єднання локальних траєкторій у складну структуру – дивний атрактор «подвійний завихрень» (Double Scroll). Саме цей режим, завдяки своїй топологічній складності та високій ентропії, був обраний для генерації псевдовипадкових послідовностей у розробленій системі шифрування.

Динаміка такого атрактора характеризується вираженою неперіодичністю та нестійкістю траєкторій, що зумовлює експоненціальну чутливість системи до мінімальних флуктуацій параметрів. Ключовими ознаками такого режиму, що підтверджують його хаотичну природу, є неперервний (суцільний) частотний спектр та стрімке згасання автокореляційної функції в часі.

З точки зору криптографічного захисту, ці властивості забезпечують фундаментальну непередбачуваність генерованих послідовностей. Будь-яка похибка у визначенні початкових умов або параметрів системи через короткий проміжок часу призводить до значної розбіжності між прогнозованою та реальною траєкторіями. Це робить практично неможливим відновлення секретного ключа методами лінійного або диференціального аналізу, оскільки детермінована природа системи нівелюється її топологічною складністю.

Одним із ключових параметрів, що генеруються математичною моделлю у безрозмірній формі, є часова залежність координати x. Хаотичний характер змін даної змінної дозволяє використовувати її як основу для формування криптографічної гами. У сучасній криптосистемах на основі динамічного хаосу виділяють три базові методи шифрування:

- Хаотичне маскування – пряме підсумовування інформаційного сигналу з хаотичною послідовністю.
- Перемикання режимів (Chaos Shift Keying) – кодування логічних станів («0» та «1») різними типами хаотичних сигналів або параметрами різних координат (наприклад, x та y).
- Нелінійне підмішування – інтеграція інформаційного повідомлення безпосередньо у структуру диференціальних рівнянь, що змінює динаміку самого атрактора.

У межах даного дослідження реалізовано алгоритм хаотичного маскування. Для досягнення статистичних характеристик, максимально наближених до істинно випадкових послідовностей, замість прямого використання амплітудних значень застосовано метод динамічного зрізу.

Цей підхід полягає у вибірковому отриманні значень фазової координати x через нерегулярні проміжки часу або шляхом екстракції лише певних розрядів цифрового представлення числа. Така обробка дозволяє нівелювати детерміновану природу генератора та суттєво підвищити складність криптоаналізу для потенційного зловмисника.

Під час проєктування програмного комплексу було застосовано методи об'єктно-орієнтованого аналізу та дизайну, що дозволило структурувати систему як сукупність взаємодіючих об'єктів. Цей підхід забезпечує розгляд предметної області через логічні сутності, де основна увага при аналізі приділяється визначенню об'єктів у термінах криптографічного захисту та нелінійної динаміки. У процесі проєктування визначено логічні програмні об'єкти, які реалізовані засобами об'єктно-орієнтованої мови програмування та включають відповідні атрибути (параметри моделі Чуа) і методи (алгоритми чисельного інтегрування та перетворення даних). Етап конструювання забезпечив безпосередню реалізацію розроблених класів та компонентів, що гарантує розширюваність та модульність системи. Основні функціональні можливості розробленого програмного забезпечення та сценарії взаємодії користувача з системою відображені на діаграмі варіантів використання, яка наведена на рисунку 2.

Варіант використання визначає функціональну можливість системи, що дозволяє користувачу отримати конкретний вимірюваний результат шляхом типової взаємодії з програмним комплексом [20]. У контексті даної роботи ключовим сценарієм є функція «Розшифрувати текст», метою якої є відновлення вихідного повідомлення за допомогою хаотичної гами.

Діючою особою (актором) виступає користувач додатка. Для коректного виконання операції необхідне дотримання попередніх умов: наявність встановленого ключа з'єднання та валідного сеансового ключа. Процес активується за командою користувача на перевірку вхідного буфера зашифрованих даних.

Основний потік подій включає наступні кроки:

1. Налаштування криптосистемою параметрів і внутрішнього стану генератора хаосу.
2. Отримання вхідного масиву зашифрованих даних.
3. Дешифрування інформаційного потоку шляхом синхронної генерації хаотичної траєкторії.
4. Верифікація цілісності даних через перевірку контрольної суми.
5. Виведення відновленого тексту на інтерфейс користувача.

Альтернативні сценарії обробки помилок:

- Відсутність ключа з'єднання: повернення коду помилки про некоректні параметри ініціалізації.
- Помилка сеансового ключа: формування сповіщення про неможливість синхронізації генераторів.
- Збій при отриманні даних: реєстрація помилки мережевого обміну або доступу до пам'яті.
- Порушення цілісності (Checksum error): повернення коду помилки про пошкодження блоку тексту, що вказує на розсинхронізацію або втручання в канал зв'язку.

Таким чином, детальний розгляд сценарію «Розшифрувати текст» дозволяє формалізувати логіку роботи модуля-приймача в умовах програмної реалізації хаотичної криптосистеми.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

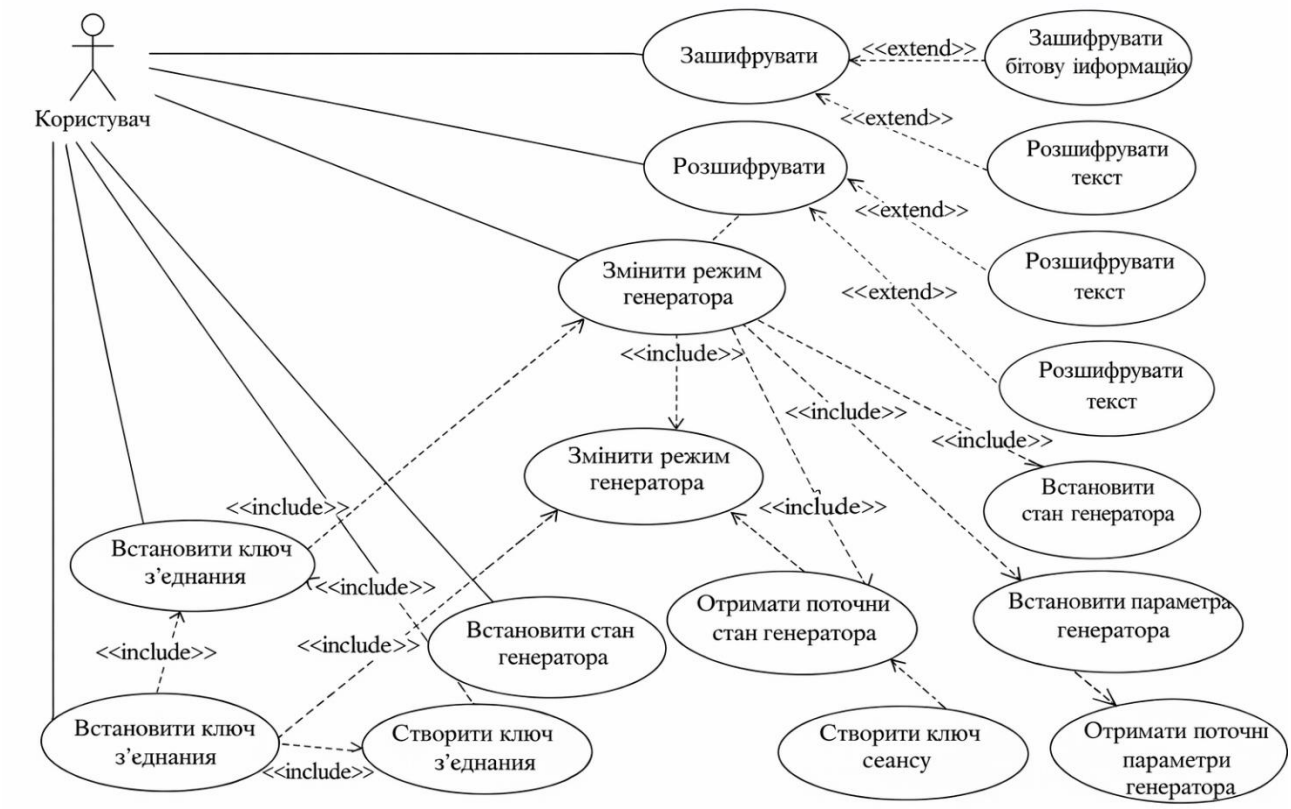

Рис. 2 – Діаграма варіантів використання

Об'єктно-орієнтована архітектура програмного комплексу базується на декомпозиції системи на окремі класи, кожен з яких відповідає за конкретний аспект функціонування моделі. Діаграма класів призначена для візуалізації структури цих класів, визначення їхніх атрибутів, методів, а також типів взаємозв'язків та ієрархії взаємодії між ними.

Проєктне рішення передбачає поділ обчислювальної логіки (чисельне розв'язання системи диференціальних рівнянь Чуа) та криптографічної обробки даних (генерування гами та маскування інформаційного сигналу). Класи, що забезпечують стабільне функціонування генератора хаосу та інтегрованої криптосистеми, а також логіку їхньої взаємодії, представлені на діаграмі класів на рисунку 3.

Аналіз структури класів дозволяє простежити архітектурні зв'язки між компонентами, що забезпечують функціонування криптосистеми, а також визначити специфікацію структур для зберігання параметрів хаотичного процесу.

Для забезпечення гнучкості обробки даних реалізовано механізм перевантаження методів: функція *Encrypt* адаптована для роботи як з текстовими, так і з бінарними (бітовими) типами даних. Це зумовлено необхідністю застосування різних алгоритмічних підходів до кодування інформації залежно від її формату при збереженні єдиного інтерфейсу керування.

Клас *Encryptor* реалізований із дотриманням принципу інкапсуляції. Він містить об'єкт *EncrGen* класу *Generator* у закритій секції. Поля цього об'єкта, як і сам екземпляр генератора, захищені від прямого зовнішнього доступу. Будь-яка взаємодія з параметрами хаотичної системи можлива лише через відкриті (*public*) методи класу *Encryptor*. Таке архітектурне рішення виключає некоректну зміну внутрішніх робочих даних об'єкта *EncrGen* та гарантує стабільність формування хаотичної гами під час сеансу зв'язку.

Діаграма послідовності призначена для відображення набору об'єктів на єдиній часовій осі їхнього життєвого циклу (створення – діяльність – знищення) та логіки їхньої взаємодії (надсилання запитів та отримання відповідей). Вона дозволяє детально проаналізувати динаміку роботи системи та хронологію обміну повідомленнями між її компонентами.

Процес взаємодії об'єктів для розглянутого варіанта використання «Розшифрувати текст», що демонструє етапи ініціалізації генератора, запиту хаотичної гами та верифікації даних, представлений на рис. 4.

p-ISSN: 2225-6733; e-ISSN: 2519-271X

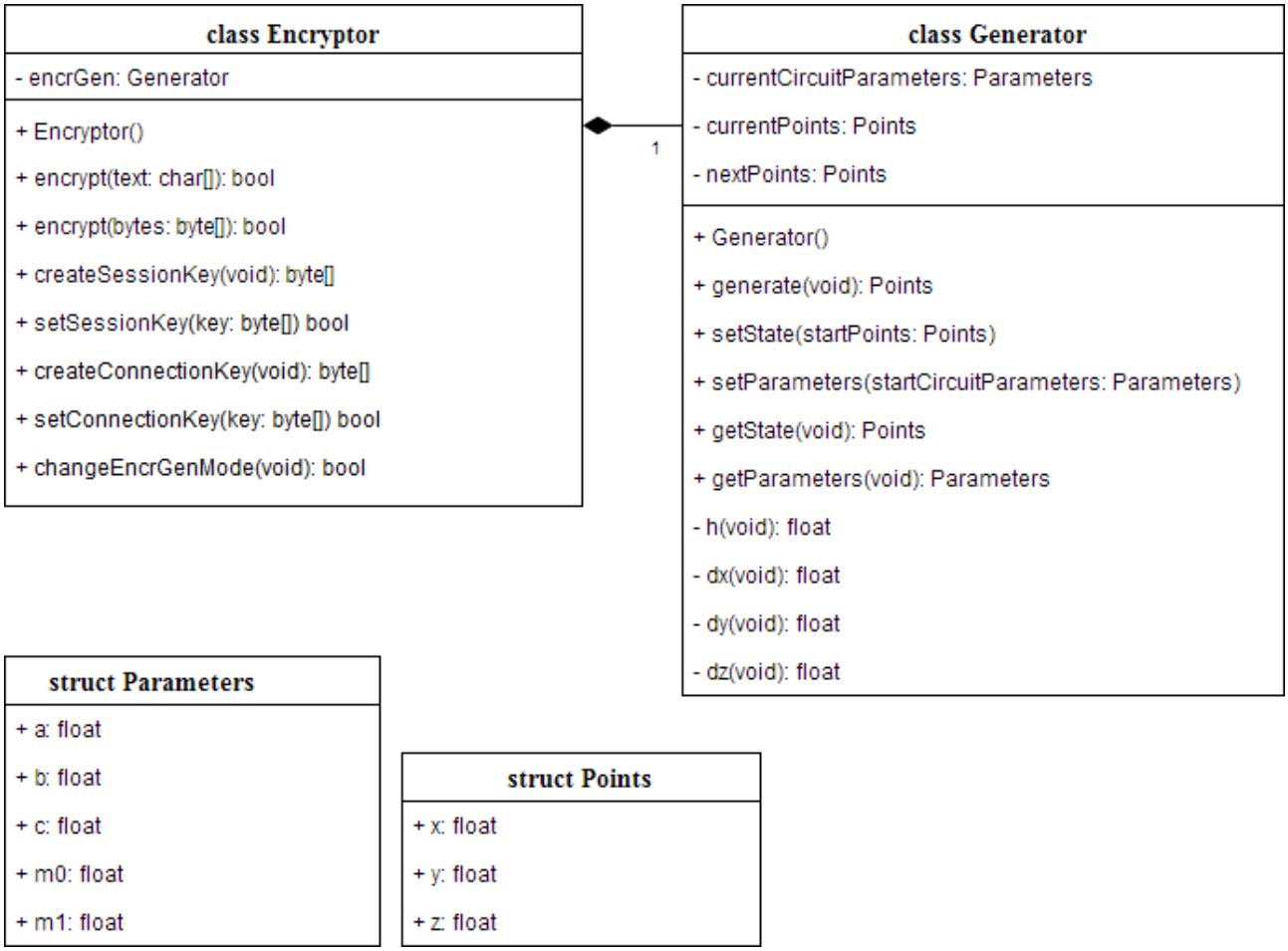

Рис. 3 – Діаграма класів

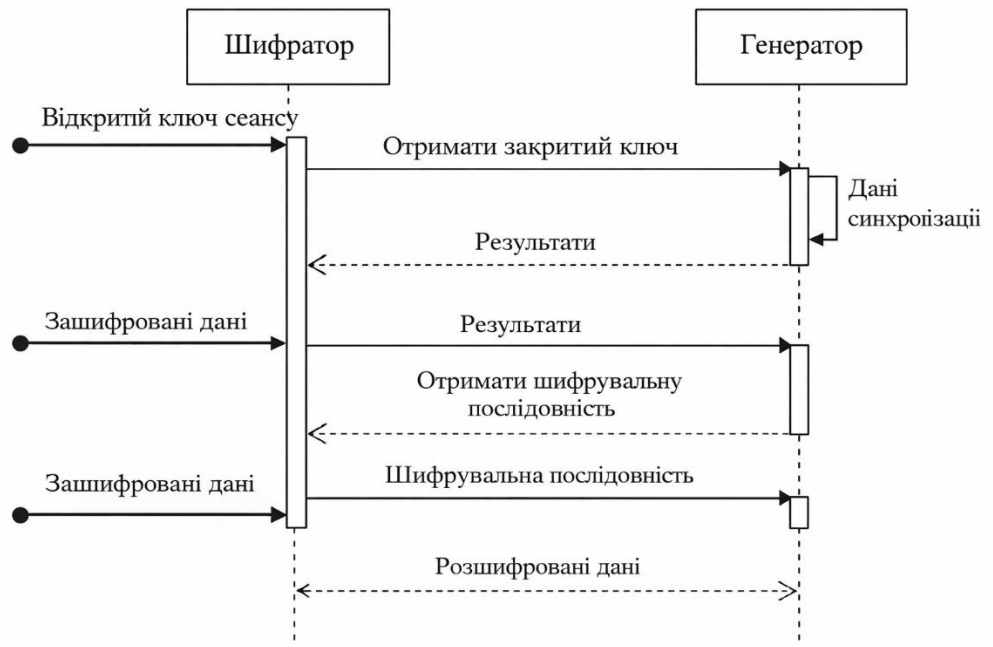

Рис. 4 – Процес взаємодії об'єктів для розглянутого варіанта використання «Розшифрувати текст»

Для чисельного розв'язання системи диференціальних рівнянь, що описують динаміку генератора хаосу, у класі *Generator* використано метод Рунге-Кутти четвертого порядку. Вибір даного методу зумовлений необхідністю забезпечення високої точності обчислень, оскільки хаотичні системи мають експоненціальну чутливість до накопичення похибок.

Алгоритм передбачає ітераційне обчислення значень фазових координат *x, y, z* з фіксованим кроком інтегрування. На кожній ітерації програма розраховує чотири проміжні коефіцієнти, що дозволяє мінімізувати локальну похибку та забезпечити стабільність хаотичного атрактора.

Програмна реалізація методу дозволяє отримувати детерміновану послідовність значень, яка є ідентичною як на стороні передавача, так і на стороні приймача за умови збігу початкових значень (ключів).

Це завершує архітектурну побудову системи: від математичної моделі та об'єктно-орієнтованої структури класів до конкретного обчислювального алгоритму. Отримана таким чином хаотична послідовність після обробки методом зрізу передається в метод *Encrypt* класу *Encryptor* для виконання операцій криптографічного маскування.

Висновки

У статті розроблено та досліджено об'єктно-орієнтовану імітаційну модель нелінійного осцилятора Чуа для генерації псевдовипадкових послідовностей. На основі проведеного дослідження сформульовано такі висновки:

1. Обґрунтовано вибір системи Чуа як базового генератора завдяки її топологічній складності та здатності формувати атрактор типу «Double Scroll» при мінімальній кількості параметрів. Введення додаткового керуючого коефіцієнта c розширює область існування хаотичних режимів і забезпечує гнучке управління генератором.
2. Забезпечено високу точність моделювання хаотичної динаміки в дискретному середовищі за допомогою методу Рунге–Кутти 4-го порядку, що гарантує детерміновану повторюваність траєкторій на стороні передавача та приймача – критично для синхронної криптографічної обробки.
3. Реалізовано гнучку об'єктно-орієнтовану архітектуру (UML), у якій логіка генератора та модуль Encryptor чітко розділені. Інкапсуляція параметрів генератора та механізм перевантаження методів Encrypt забезпечують захист внутрішніх даних та масштабованість системи для різних типів інформації.
4. Проаналізовано вплив параметрів системи та початкових умов на стабільність хаотичного режиму. Дослідження підтвердило, що навіть мінімальні зміни початкових значень значно змінюють траєкторію атрактора, що забезпечує непередбачуваність генерованого потоку.
5. Розроблена модель може бути інтегрована в сучасні інформаційно-комунікаційні системи як програмний компонент для захищеної передачі даних у цифровому середовищі.

Перелік використаних джерел

[1] A New 3D Chaotic System with Hidden Attractor: Dynamics, Circuit Implementation and Its Application in Cryptography / A. Sambas et al. *IEEE Access*. 2022. Vol. 10. Pp. 64610–64627. DOI: https://doi.org/10.1109/ACCESS.2022.3181424.

[2] Hyperchaotic System for Secure Communication: A Modified 4D Model and its Dynamics / Aldwoah K., Hassan E. I., Alsharafi M. & Alharbi A. F. *Journal of Nonlinear Mathematical Physics*. 2025. Vol. 32. Article 90. DOI: https://doi.org/10.1007/s44198-025-00348-8.

[3] Enhanced chaotic pseudorandom number generation using multiple Bernoulli maps with Field Programmable Gate Array optimizations / L. Palacios-Luengas et al. *Information*. 2024. Vol. 15. No. 11. Article 667. DOI: https://doi.org/10.3390/info15110667.

[4] Bhattacharjee K., Das S. A Search for Good Pseudo-Random Number Generators: Survey and Empirical Studies. *Computer Science Review*. 2022. Vol. 45. Article 100471. DOI: https://doi.org/10.1016/j.cosrev.2022.100471.

[5] El-den B. M., Raslan W. A., Abdullah A. A. Even Symmetric Chaotic and Skewed Maps as a Technique in Video Encryption. *EURASIP Journal on Advances in Signal Processing*. 2023. Vol. 2023, Article 40. DOI: https://doi.org/10.1186/s13634-023-01003-4.

[6] Zhang J., Lu Z., Li M. Research on an effective image encryption scheme based on hyper-chaos using global bit permutation. *Technology and Health Care*. 2020. Vol. 28, No. S1. Pp. 313–323. DOI: https://doi.org/10.3233/THC-209030.

[7] Patidar V., Singh T. A Novel Approach to Pseudorandom Number Generation Using Hamiltonian Conservative Chaotic Systems. *Frontiers in Physics*. 2025. Vol. 13. Article 1553389. DOI: https://doi.org/10.3389/fphy.2025.1553389.

[8] Alawida M. Enhancing logistic chaotic map for improved cryptographic security in random number generation. *Journal of Information Security and Applications*. 2024. Vol. 80. Article 103685. DOI: https://doi.org/10.1016/j.jisa.2023.103685.

[9] A Pseudorandom Number Generator Based on the Chaotic Map and Quantum Random Walks / Zhao W., Chang Z., Ma C., Shen Z. *Entropy*. 2023. Vol. 25, no. 1. Article 166. DOI: https://doi.org/10.3390/e25010166.

[10] Sun F., Lv Z., Wang C. Pseudo-Random Number Generation Based on Spatial Chaotic Map of Logistic Type and Its Cryptographic Application. *International Journal of Modern Physics C*. 2025. Vol. 36, no. 1.

Article 2450172. DOI: https://doi.org/10.1142/S0129183124501729.
[11] Özpolat E., Çelik V., Gülten A. Hyperchaotic System-Based PRNG and S-Box Design for a Novel Secure Image Encryption. *Entropy*. 2025. Vol. 27, no. 3. Article 299. DOI: https://doi.org/10.3390/e27030299.
[12] Shi Y., Deng Y. Hybrid Control of a Digital Baker Map with Application to a Pseudo-Random Number Generator. *Entropy*. 2021. Vol. 23, no. 5. Article 578. DOI: https://doi.org/10.3390/e23050578.
[13] Hardware Pseudorandom Number Generator Using Stochastic Computing and Logistic Map / J. Liu et al. *Micromachines*. 2021. Vol. 12, no. 1. Article 31. DOI: https://doi.org/10.3390/mi12010031.
[14] Pseudorandom Number Generator Based on Novel 2D Hénon–Sine Hyperchaotic Map With Microcontroller Implementation / D. Murillo-Escobar et al. *Nonlinear Dynamics*. 2023. Vol. 111. Pp. 6773–6789. DOI: https://doi.org/10.1007/s11071-022-08101-2.
[15] Quantum walks with cascaded discrete times with induced chaotic dynamics and cryptographic applications / Abd El-Latif A. A., Abd-El-Atti B., Amin M., Iliyasu A. M. *Scientific Reports*. 2020. Vol. 10. Article 1930. DOI: https://doi.org/10.1038/s41598-020-58636-w.
[16] High-security multidimensional data protection system based on a Hartley algorithm-based chaotic scheme / J. Cui et al. *Optics Express*. 2024. Vol. 32, no. 13. Pp. 22295–22312. DOI: https://doi.org/10.1364/OE.522606.
[17] Quantum random number generators / Jacak M. M., Jóźwiak P., Niemczuk J., Jacak J. E. *Scientific Reports*. 2021. Vol. 11. Article 16104. DOI: https://doi.org/10.1038/s41598-021-95388-7.
[18] Lian S., Sun J., Wang Z. Implementation and practical problems of chaos-based cryptography. *Journal of Information Security and Applications*. 2020. Vol. 50. Article 102421. DOI: https://doi.org/10.1016/j.jisa.2019.102421.
[19] Learned pseudo-random number generator: WGAN-GP for generating statistically sound random numbers / Okada K., Endo K., Yasuoka K., Kurabayashi S. *PLOS ONE*. 2023. Vol. 18, no. 6. Article e0287025. DOI: https://doi.org/10.1371/journal.pone.0287025.
[20] Design of New Chaotic System With Hyperbolic Sine Function Based on Pseudo-Random Number Generation for Medical Image Encryption / R. Ramar et al. *Journal of Nonlinear Mathematical Physics*. 2025. Vol. 32. Article 52. DOI: https://doi.org/10.1007/s44198-025-00308-2.

SIMULATION MODEL OF AN ELECTRONIC NONLINEAR OSCILLATOR FOR HIGH-ENTROPY SEQUENCE GENERATION IN INFORMATION SECURITY PROBLEMS

Levytska T.O. *PhD (Engineering), associate professor, SHEI «Priazovskyi state technical university», Dnipro, ORCID: https://orcid.org/0000-0003-3359-1313, e-mail: levitskaya_t_a@pstu.edu;*

Nosovska S.Ye. *senior lecturer, SHEI «Priazovskyi state technical university», Dnipro, ORCID: https://orcid.org/0000-0002-6176-6101, e-mail: nosovska_s_e@pstu.edu*

Modern information security systems and protected communication channels require sources of high entropy and resistance to predictability. This paper proposes an approach for modeling and software implementation of an electronic nonlinear oscillator as a source of pseudorandom sequences for cryptographic applications. The mathematical framework is based on the Chua oscillator model, which allows investigating the dynamics of third-order nonlinear systems and studying the conditions for the onset of deterministic chaos. The modified system of equations includes an additional control coefficient, which extends the range of chaotic attractors and provides flexible management of oscillation regimes. Numerical simulation of the system dynamics was performed using the fourth-order Runge–Kutta method, ensuring high-precision reproduction of trajectories and stability of the chaotic regime under exponential sensitivity to initial conditions. For software implementation, an object-oriented approach was applied, structuring the system as a set of interacting objects, including the chaos generator and the cryptographic data processing module. The use of UML class and sequence diagrams ensures modularity, scalability, and clear component interaction. Special attention is given to methods for generating chaotic keystreams and their use for cryptographic signal masking, guaranteeing the unpredictability of output sequences. The system's dynamic regimes were analyzed, a «parameter–regime» matrix was constructed, and the influence of initial conditions and system parameters on the stability of the chaotic regime was determined, which is critical for reliable cryptographic protection. Thus, the study integrates mathematical modeling, numerical methods, and object-oriented software architecture to create a robust source of high-quality pseudorandom sequences suitable for modern cryptographic applications and secure information transmission.

Keywords: *information security; simulation modeling; nonlinear oscillator; deterministic chaos; pseudorandom sequences; Runge–Kutta method; UML design; cryptographic robustness.*

References

[1] A. Sambas, S. Vaidyanathan, and X. Zhang, "A New 3D Chaotic System with Hidden Attractor: Dynamics, Circuit Implementation and Its Application in Cryptography," *IEEE Access*, vol. 10, pp. 64610–64627, 2022. **doi: 10.1109/ACCESS.2022.3181424**.

[2] K. Aldwoah, E. I. Hassan, M. Alsharafi, and A. F. Alharbi, "Hyperchaotic System for Secure Communication: A Modified 4D Model and its Dynamics," *Journal of Nonlinear Mathematical Physics*, vol. 32, article 90, 2025. **doi: 10.1007/s44198-025-00348-8**.

[3] L. Palacios-Luengas, R. C. Medina-Ramírez, R. Marcelín-Jiménez, E. Rodriguez-Colina, F. R. Castillo-Soria, and R. Vázquez-Medina, "Enhanced chaotic pseudorandom number generation using multiple Bernoulli maps with Field Programmable Gate Array optimizations," *Information*, 2024. vol. 15, no. 11, article 667, 2024. **doi: 10.3390/info15110667**.

[4] K. Bhattacharjee, and S. Das, "A Search for Good Pseudo-Random Number Generators: Survey and Empirical Studies," *Computer Science Review*, vol. 45, article 100471, 2022. **doi: 10.1016/j.cosrev.2022.100471**.

[5] B. M. El-den, W. A. Raslan, and A. A. Abdullah, "Even Symmetric Chaotic and Skewed Maps as a Technique in Video Encryption," *EURASIP Journal on Advances in Signal Processing*, vol. 2023, article 40, 2023. **doi: 10.1186/s13634-023-01003-4**.

[6] J. Zhang, Z. Lu, and M. Li, "Research on an effective image encryption scheme based on hyper-chaos using global bit permutation," *Technology and Health Care*, vol. 28, no. s1, pp. 313–323, 2020. **doi: 10.3233/THC-209030**.

[7] V. Patidar, and T. Singh, "A Novel Approach to Pseudorandom Number Generation Using Hamiltonian Conservative Chaotic Systems," *Frontiers in Physics*, vol. 13, article 1553389, 2025. **doi: 10.3389/fphy.2025.1553389**.

[8] M. Alawida, "Enhancing logistic chaotic map for improved cryptographic security in random number generation," *Journal of Information Security and Applications*, vol. 80, article 103685, 2024. **doi: 10.1016/j.jisa.2023.103685**.

[9] W. Zhao, Z. Chang, C. Ma, and Z. Shen, "A Pseudorandom Number Generator Based on the Chaotic Map and Quantum Random Walks," *Entropy*, vol. 25, no. 1, article 166, 2023. **doi: 10.3390/e25010166**.

[10] F. Sun, Z. Lv, and C. Wang, "Pseudo-Random Number Generation Based on Spatial Chaotic Map of Logistic Type and Its Cryptographic Application," *International Journal of Modern Physics C*, vol. 35, no. 2, article 2450024, 2024. **doi: 10.1142/S0129183124500246**.

[11] E. Özpolat, V. Çelik, and A. Gülten, "Hyperchaotic System-Based PRNG and S-Box Design for a Novel Secure Image Encryption," *Entropy*, vol. 27, no. 3, article 299, 2025. **doi: 10.3390/e27030299**.

[12] Y. Shi, and Y. Deng, "Hybrid Control of a Digital Baker Map with Application to a Pseudo-Random Number Generator," *Entropy*, vol. 23, no. 5, article 578, 2024. **doi: 10.3390/e23050578**.

[13] J. Liu et al., "Hardware Pseudorandom Number Generator Using Stochastic Computing and Logistic Map," *Micromachines*, vol. 12, no. 1, article 31, 2021. **doi: 10.3390/mi12010031**.

[14] D. Murillo-Escobar, M. Á. Murillo-Escobar, C. Cruz-Hernández, and L. Cardoza-Avendaño, "Pseudorandom Number Generator Based on Novel 2D Hénon–Sine Hyperchaotic Map With Microcontroller Implementation," *Nonlinear Dynamics*, vol. 111, pp. 6773–6789, 2023. **doi: 10.1007/s11071-022-08101-2**.

[15] A. A. Abd El-Latif, B. Abd-El-Atti, M. Amin, and A. M. Iliyasu, "Quantum walks with cascaded discrete times with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, article 1930, 2020. **doi: 10.1038/s41598-020-58636-w**.

[16] J. Cui et al., "High-security multidimensional data protection system based on a Hartley algorithm-based chaotic scheme," *Optics Express*, vol. 32, no. 13, pp. 22295–22312, 2024. **doi: 10.1364/OE.522606**.

[17] M. M. Jacak, P. Jóźwiak, J. Niemczuk, and J. E. Jacak, "Quantum random number generators," *Scientific Reports*, vol. 11, article 16104, 2021. **doi: 10.1038/s41598-021-95388-7**.

[18] S. Lian, J. Sun, and Z. Wang, "Implementation and practical problems of chaos-based cryptography," *Journal of Information Security and Applications*, vol. 50, article 102421, 2020. **doi: 10.1016/j.jisa.2019.102421**.

[19] K. Okada, K. Endo, K. Yasuoka, and S. Kurabayashi, "Learned pseudo-random number generator: WGAN-GP for generating statistically sound random numbers," *PLOS ONE*, vol. 18, no. 6, article e0287025, 2023. **doi: 10.1371/journal.pone.0287025**.

[20] R. Ramar et al., "Design of New Chaotic System With Hyperbolic Sine Function Based on Pseudo-Random Number Generation for Medical Image Encryption," *Journal of Nonlinear Mathematical Physics*, vol. 32, article 52, 2025. **doi: 10.1007/s44198-025-00308-2**.

Стаття надійшла 24.01.2026
Стаття прийнята 26.02.2026
Стаття опублікована 26.03.2026

Цитуйте цю статтю як: Левицька Т. О., Носовська С.Є. Імітаційна модель електронного нелінійного осцилятора для генерації високоентропійних послідовностей у задачах захисту інформації. *Вісник Приазовського державного технічного університету. Серія: Технічні науки*. 2026. Вип. 53, том 1. С. 76–84. DOI: https://doi.org/10.31498/2225-6733.53.1.2026.359779.