Вінницький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет інформаційних електронних систем
(повне найменування інституту, назва факультету (відділення))

Кафедра інформаційних радіоелектронних технологій і систем
(повна назва кафедри (предметної. циклової комісії))

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МІКРОЕЛЕКТРОННИЙ ПРИСТРІЙ ДЛЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ»

Виконав: студ. 2-го курсу, групи МНТ-22м
спеціальності 153 Мікро- та наносистемна техніка
(шифр і назва напряму підготовки, спеціальності)
_____ Штефанеса С.С.
(прізвище та ініціали)

Керівник: д.т.н., професор, проф. каф. ІРТС
_____ Семенов А.О.
(прізвище та ініціали)
«18» 12 2023 р.

Опонент: д.т.н., доцент, професор каф. ІКСТ
_____ Михалевський Д.В.
(прізвище та ініціали)
«19» 12 2023 р.

Допущено до захисту
Завідувач кафедри ІРТС
д.т.н., проф. Осадчук О.В.
(прізвище та ініціали)
«20» 12 2023 р.

Вінниця ВНТУ - 2023 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інформаційних радіоелектронних технологій і систем
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань – 15 Автоматизація та приладобудування
Спеціальність – 153 Мікро- та наносистемна техніка
Освітньо-професійна програма – Мікро- та наносистемна техніка

ЗАТВЕРДЖУЮ
Завідувач кафедри ІРТС
д.т.н., проф. Осадчук О.В.
«16» вересня 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Штефанесі Сергію Сергійовичу
(прізвище, ім'я. по батькові)

1. Тема роботи «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань»
керівник роботи д.т.н., проф., проф. кафедри ІРТС Семенов А.О.
(прізвище, ім'я. по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «18» 09.2023 р. №247.
2. Строк подання студентом роботи 15.12.2023р.
3. Вихідні дані до роботи: Робочий діапазон частот від 100 кГц до 16,65 МГц; діапазон частот інформаційних сигналів від 300 Гц до 5 кГц; напруга живлення 9 В; потужність споживання не більше 100 мВт; час перемикання не більше 25 мс; середнє напрацювання на відмову, не менше 10000 годин.
4. Зміст текстової частини: Вступ. Аналіз методів захисту інформації з використанням генератора хаотичних коливань. Використання генератора хаотичних коливань в системах захисту інформації. Розроблення генератора хаотичних коливань на приладі з від'ємним диференційним опором. Експериментальні дослідження пристрою захисту інформації з використанням генератора хаосу. Економічна частина. Охорона праці та безпека в надзвичайних ситуаціях. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень): Класифікація шифрів. Хаотичне маскування. Перемикання хаотичних режимів. Нелінійне підмішування сигналів. Рознесення сигналів. Схема генератора Чуа. Вольт-амперна характеристика нелінійного елемента. Схема маскування хаотичним сигналом. Паралельне з'єднання двох кусково-лінійних резисторів. Принципова схема системи Чуа. Додаткові ОП включені в схему для усунення впливу вимірювальних приладів на динаміку системи Чуа. Реалізація схеми генератора Чуа в програмному пакеті Micro-Cap. Часова діаграма сигналу на виході генератора. Спектральні характеристики генерованих схемою Чуа сигналів. Структурна схема генератора хаосу.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	виконання прийняв
Основна частина	д.т.н., проф., проф. каф. ІРТС Семенов А.О.		
Економічна частина	доцент каф. ЕПВМ, доцент, к.е.н., Кавецький В.В.		
Охорона праці та безпека в надзвичайних ситуаціях	професор кафедри БЖДПБ, професор, д.п.н., Дембіцька С.В.		

7. Дата видачі завдання 17.09.2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір, узгодження та затвердження тем МКР на випусковій кафедрі.	02.09.2023-07.09.2023	
2.	Огляд та аналіз літературних джерел.	08.09.2023-17.09.2023	
3.	Затвердження тем по ВНТУ. Розробка завдання на МКР.	18.09.2023-27.09.2023	
4.	Попередня розробка основних розділів. Аналіз вирішення поставленої задачі. Розробка структурної схеми та технічних рішень.	28.09.2023-10.10.2023	
5.	Математичне моделювання та електричні розрахунки. Експериментальне дослідження.	11.10.2023-26.10.2023	
6.	Розробка графічної частини МКР.	27.10.2022-12.11.2022	
7.	Економічна частина.	13.11.2023-16.11.2023	
8.	Охорона праці (ОП).	17.11.2022-22.11.2022	
9.	Оформлення пояснювальної записки та графічної частини.	23.11.2023-28.11.2023	
10.	Нормоконтроль.	29.11.2023-30.11.2023	
11.	Попередній захист МКР, доопрацювання, рецензування МКР.	01.12.2023	
12.	Захист МКР ЕК.	21.12.2023-22.12.2023	

Студент _____ (підпис) Штефанеса С.С.

Керівник роботи _____ (підпис) Семенов А.О.

АНОТАЦІЯ

УДК 621.382

Штефанеса С.С. Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань: магістерська кваліфікаційна робота – Вінниця: ВНТУ 2023 р. – 132 стор., 51 рис., 41 бібл., 15 табл. – українською мовою.

Магістерська кваліфікаційні робота присвячена захисту інформації з використанням генератора хаотичних коливань, оскільки захист інформації від несанкціонованого доступу є однією з найбільш актуальних задач в телекомунікаціях та радіотехніці. Головна особливість детермінованих хаотичних коливань полягає в їх великої інформаційної ємності, а можливість їх застосування в системах передачі інформації пов'язана, перш за все з тим, що існує цілком певний детермінований алгоритм, на підставі якого можна відтворити необхідні хаотичні коливання будь-яку кількість разів, необхідну для їх технічного використання.

В магістерській кваліфікаційній роботі проводилась розробка моделей генераторів детермінованого хаосу та дослідження їх властивостей є актуальним завданням, перш за все для створення телекомунікаційних та радіотехнічних систем, а також для всіх галузей науки і техніки, де можливе в перспективі застосування хаотичних коливань.

Для дослідження існуючої моделі генератора хаосу було використано методи математичного моделювання та комп'ютерного моделювання. Наукова новизна одержаних результатів полягає в подальшому розвитку теоретичних засад детермінованого хаосу для СЗІ, що забезпечило підвищення ефективності цього процесу в цілому.

У розділі «Охорона праці та безпека у надзвичайних ситуаціях» проведений аналіз умов праці в приміщенні, в якому виконується робота, а також проведено оцінку безпеки в разі дії електромагнітного випромінювання досліджуваного генератора хаотичних коливань.

Економічна частина включає розрахунок кошторису витрат на проведення роботи з даної теми і ефективності отриманих в результаті виконання результатів.

Ключові слова: генератор хаотичних коливань, детермінований хаос, генератор коливань, генератор хаосу.

ABSTRACT

Stefanes S.S. A microelectronic device for technical protection of information using a generator of chaotic oscillations: master's qualification thesis - Vinnytsia: VNTU 2023 - 117 pages, 51 figures, 41 bibl., 15 tables. - in the Ukrainian language.

The master's thesis is devoted to the protection of information using a generator of chaotic oscillations, since the protection of information from unauthorized access is one of the most urgent tasks in telecommunications and radio engineering. The main feature of deterministic chaotic oscillations is their large information capacity, and the possibility of their application in information transmission systems is connected, first of all, with the fact that there is a completely certain deterministic algorithm, on the basis of which the necessary chaotic oscillations can be reproduced any number of times , necessary for their technical use.

In the master's qualification work, the development of models of deterministic chaos generators was carried out, and the study of their properties is an urgent task, first of all, for the creation of telecommunication and radio engineering systems, as well as for all fields of science and technology, where the application of chaotic oscillations is possible in the future.

The methods of mathematical modeling and computer simulation were used to study the existing model of the chaos generator. The scientific novelty of the obtained results lies in the further development of the theoretical foundations of deterministic chaos for SHI, which ensured an increase in the efficiency of this process as a whole.

In the section "Occupational protection and safety in emergency situations" an analysis of working conditions in the room where the work is carried out was carried out, as well as an assessment of safety in the event of electromagnetic radiation of the investigated generator of chaotic oscillations was carried out.

The economic part includes the calculation of the cost estimate for the work on this topic and the efficiency of the results obtained as a result of the implementation.

Key words: chaotic oscillation generator, deterministic chaos, oscillation generator, chaos generator.

ЗМІСТ

ВСТУП

Актуальність теми.

В даний час в умовах швидкого розвитку інформаційних технологій та вдосконалення технічних засобів обробки, передачі та зберігання інформації, зростає не тільки кількість нових завдань у цій області, але і кількість технічних рішень вже відомих, традиційних завдань. Для цього ведеться пошук і створення нових технічних засобів. Актуальним завданням була і продовжує залишатися, зокрема, задача забезпечення конфіденційності при передачі інформації. Один з напрямків вирішення цього завдання пов'язаний з використанням детермінованого хаосу. Цей перспективний напрям у техніці зв'язку, здатний привести до нових результатів при вирішенні задач конфіденційності передачі інформації. Кількість робіт, присвячених застосуванню в системах зв'язку хаотичних коливань, постійно зростає. Це напрямок з'явився після того, як в результаті розвитку нелінійної динаміки було відкрито явище, назване динамічним або детермінованим хаосом. Було виявлено, що в деяких динамічних системах, при певних умовах, виникають особливого типу нелінійні коливання, спектр яких не відрізняється від спектра нормального шумового процесу, але при цьому існує певний алгоритм, використовуючи який, можна ці коливання відтворити [1].

Рішення технічної задачі створення систем зв'язку на основі детермінованого хаосу є одним із способів забезпечення конфіденційності передачі повідомлень, що вже само по собі є досить актуальним завданням. Головна особливість детермінованих хаотичних коливань полягає в їх великої інформаційної ємності, а можливість їх застосування в системах передачі інформації пов'язана, перш за все з тим, що існує цілком певний детермінований алгоритм, на підставі якого можна відтворити необхідні хаотичні коливання будь-яку кількість разів, необхідну для їх технічного використання.

Труднощі, що виникають при вирішенні технічної задачі, пов’язаної з використанням детермінованого хаосу в інформаційних технологіях, і, зокрема, в системах передачі інформації, обумовлені необхідністю отримання хаотичних коливань із заданими параметрами і питаннями їх керованості. Тому створення моделей генераторів хаосу і дослідження їх властивостей можна вважати необхідною ланкою у вирішенні технічної задачі створення систем зв’язку, що працюють на основі використання детермінованого хаосу.

Таким чином, розробка моделей генераторів детермінованого хаосу і дослідження їх властивостей є актуальним завданням, перш за все для створення телекомунікаційних систем, а також для всіх галузей науки і техніки, де можливе в перспективі застосування хаотичних коливань [2, 3].

Зв’язок роботи з науковими програмами, планами, темами.

Основні задачі роботи відповідають державним науково-технічним програмам, що визначені Законами України «Про наукову і науково-технічну діяльність», напряму інформаційні та комунікаційні технології згідно з Законом України від 12.01.2023 № 2859-IX «Пріоритетні напрями розвитку науки і техніки» та «Про пріоритетні напрями інноваційної діяльності в Україні».

Метою роботи розроблення та дослідження притрою захисту інформації в радіотехніничх і телекомунікаційних системах з використання генератора хаотичних коливань.

Для досягнення поставленої мети в роботі необхідно вирішити наступні **задачі**:

- проаналізувати існуючі методи захисту інформації;
- проаналізувати використання моделей генераторів хаосу в системах хахисту інформації;
- провести розрахунки та комп’ютерне моделювання в програмному середовищі Micro-Cap генератора хаотичних коливань на базі приладів із від’ємним диференційним опором;
- дослідити різні види коливних процесів генератора хаосу, що утворюються шляхом зміни значень її параметрів.

- дослідити захист інформації в аналоговій системі передачі інформації з використанням генератора хаотичних коливань на приладі з від'ємним диференційним опором;
- проаналізувати одержані результати.

Об'єктом дослідження є процеси захисту інформації з використанням детермінованого хаосу в динамічних системах.

Предметом дослідження є схема генератора хаосу та методи захисту інформації з використанням детермінованого хаосу в динамічних системах.

Методи дослідження. Теоретичний аналіз, математичне моделювання, фазові портрети, синхронізація, біфуркаційні явища. Для дослідження існуючої моделі генератора хаосу було використано методи математичного моделювання та комп'ютерного моделювання. Наукова новизна одержаних результатів полягає в подальшому розвитку теоретичних засад детермінованого хаосу для СЗІ, що забезпечило підвищення ефективності цього процесу в цілому.

Практичне значення одержаних результатів. Отримані результати дали змогу дослідити схему генератора хаосу. Параметри коливань в експериментальних зразках генераторів коливань вказують на перспективу їх застосування в системах зв'язку з використанням хаотичних процесів.

Особистий внесок здобувача. Основні положення і результати магістерської кваліфікаційної роботи отримані автором самостійно.

Структура і обсяг роботи. Магістерська кваліфікаційна робота складається зі вступу, 6 розділів, висновків, додатків та списку використаних джерел.

1 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ

Із збільшенням кількості інформації та її ролі в інноваційному світі, актуальніше стає завдання захисту інформації від несанкціонованого доступу до неї. На новому етапі розвитку технологій, доступ до будь-якої інформації, яка передається каналами зв'язку, досить легко може бути реалізований за допомогою спеціальних технічних засобів. На жаль, на даний момент на всьому ланцюжку процесів генерації, шифрування і доставки інформації до споживача є багато вузьких місць, що сприяють витоку інформації. Одним з таких прикладів може бути витік інформації з вузлів електричних каналів зв'язку у вигляді електромагнітного поля, що змінюється згідно переданої інформації. У таких випадках, природно, інформація може бути ще не закодованою, тобто незахищеною від читання вмісту сигналу, тому зловмисники дуже легко можуть отримати доступ до даної інформації. Через такі зломи прихованих даних, необхідно розробляти відповідні методи захисту інформації, що дозволяють приховувати інформаційні повідомлення при будь-яких можливих витоках. Як відомо, всі розглянуті методи захисту інформації, що містяться в сигналах, умовно можна розділити на дві категорії: перша шифрування і друга маскування. Шифрування традиційно пов'язане з алгоритмами криптографічного захисту, а маскування передбачає змішування інформаційного сигналу з шумоподібним випадковим сигналом.

1.1 Методи криптографічного захисту інформації

Криптографія вирішує проблеми пов'язані із захистом інформації шляхом їх перетворення. Вона займається проблемами аутентифікації, цілісності, конфіденційності та рядом інших з ними пов'язаних завдань. Практична криптографія вивчає методи шифрування інформацій, сертифікатами та управління ключами, створення електронного підпису. Криптоаналіз розглядає

протилежні криптографічні завдання, зокрема, несанкціоноване дешифрування даних (без знання ключа).Розділ математики, що вивчає математичні основи методів криптографії та криптоаналізу, який розглядає всі вище зазначені завдання називається криптологією.

1.1.1 Криптографічна система

Криптографічна система це вся інфраструктура, яка гарантує захист інформації (засобами обчислювальної техніки), тобто сукупність узгоджених засобів шифрування, аутентифікації, передачі ключів та інших компонент. Нехай x, k, y- кінцеві множини можливих відкритих текстів, ключів і шифрованих текстів відповідно. У більшості випадків x і y представляють собою об'єднання декартових ступенів деяких множин a і b відповідно, $X = \overset{L}{\underset{i=1}{U}} a, \quad Y = \overset{L_1}{\underset{i=1}{U}} b^i.$

Множини a і b називаються відповідно алфавітом відкритого тексту і алфавітом шифрованого тексту, відкриті та шифровані тексти записуються у вигляді послідовностей символів [6-8].

Нехай $e_k : x \to y$ – правило зашифрування на ключі $k \in K$.Позначимо множини $\{e_k : k \in K\}$ через e, а множини $\{e_k(x) : x \in X\} - e_k(x)$. Також $D_k : e_k(x) \to X$ правило розшифрування на ключі $k \in K$ множини $D_k : k \in K$.

Визначення 1. Сума $\sum_A = (x, k, y, e, d)$ даних множин, якщо виконуються наступні властивості:

1) для будь-яких $x \in X$ і $k \in K$ для яких виконується рівність $d_k(e_k(x)) = x$;

2) $y = \underset{k \subset K}{U} e_k(x)$ називаються шифром.

Шифромою називається сукупність множин можливих відкритих текстів (те, що шифрується), необхідних ключів (те, за допомогою чого шифрується), можливих шифротекстів (те, у що шифрується), правил зашифрування і правил розшифрування. Перше визначення вводить математичну (звану алгебраїчну) модель шифру, яка виявляє основні властивості реальних шифрів. Введемо

тепер імовірнісну модель шифру. Сформулюємо апріорний розподіл ймовірностей $P(x)$, $P(k)$ на множинах x і k відповідно. Так само для будь-якого $x \in X$ визначена імовірність $p_x(x) \in P(X)$ і для будь-якого $k \in K$ - імовірність $p_k \in P(k)$ причому виконуються рівності $\sum_{x \in X} p_x(x) = 1$ і $\sum_{k \in K} p_k(k) = 1$.

Коли потрібно знати розподіл $P(X)$ і $P(K)$, тоді вживаються ймовірнісні моделі $\sum_B$, що складаються з п'яти множин $\sum_B (x, k, y, e, d, P(x), P(k))$, пов'язаних станами (1) і (2) перше визначення, і двох імовірнісних розподілів. Імовірнісні характеристики шифрів використовуються лише при криптоаналізі систем.

1.1.2 Класифікація шифрів за різними ознаками

Для початкової ознаки, за допомогою якої відбувається класифікація шифрів, використовується відповідний для неї тип перетворення [9]. Коли символи відкритого тексту при шифруванні лише зміняються місцями один з одним, тут відбувається шифром перестановки. Коли частини відкритого тексту (під текстом мається на увазі будь-який вид інформації: графічний, музичний, текстовий і т.д.) змінюють деякі їх еквіваленти шифротексту, то шифр належить до класу шифрів заміни. Для покращення надійності шифрування шифрований текст, використовується для вживанням іншого шифру, може бути ще раз зашифровано за допомогою іншого шифру. Поєднання різних шифрів призводить до появи третього класу шифрів - композиційних шифрів.

Математична модель шифру заміни

Проаналізуємо модель $\sum_A = (X, K, Y, E, D)$ довільного шифру заміни. Будемо вважати, що відкритим текстом є букви алфавіту A і B відповідно: $X \subset A^*$, $Y \subset B^*$, $|A| = n$, $|B| = m$. Тут і надалі C^* виступає як множина слів кінцевої довжини в алфавіті C.

Перед зашифруванням відкритий текст спочатку зображується у вигляді послідовностей підслів, що називаються шифровеличинами. При шифруванні, шифровеличини замінюються іншими еквівалентами в шифротексті -

шифрозначеннями. Шифровеличини і шифрозначення відображають собою слова з A і B.

Нехай $U=\{u_1,...,u_N\}$ – множини даних шифровеличин, $V=\{v_1,...,v_m\}$ – множини здійснюваних шифрозначень. Ці множини повинні бути такими, щоб будь-які тексти, $x\in X$ і $y\in Y$ представлялися словами з U^*, V^*, відповідно. Вимога чіткості розшифрування несе за собою нерівність $N\geq n,\ \mathrm{N}\geq \mathrm{m},\ \mathrm{M}\geq \mathrm{N}$.

Якщо, $\mathrm{M}\geq \mathrm{N}$, множину V можна представити у вигляді злиття $V=\bigcup_{i=1}^{N} V^{(i)}$ непересічних непорожніх підмножин $V^{(i)}$.

Проаналізуємо сімейство, що складається з r таких поділів множин $V: V=\bigcup_{i=1}^{N} V_a^{(i)},\ \alpha=1,...,\mathrm{r},\ \mathrm{r}\in N$ і відповідного сімейства бієкцій $\varphi_a: U\to\{V_a^{(1)},...,V_a^{(N)}\},\ \mathrm{k}\in \mathrm{K},\ \mathrm{l}\in \mathrm{N}$ для яких $\varphi_a(u_i)=V_a^{(i)},\ \mathrm{i}=1,...,\mathrm{N}$.

А також довільне відображення $\psi: K\times N\to N_r^*$, де $N_r=\{1,2,...,r\}$, таке, що для будь-яких $k\in K,\ \mathrm{l}\in \mathrm{N}$

$$\psi(\mathrm{k,l})=\alpha_1^{(k)},\ \ \alpha_j^{(k)}\in N_r,\ \mathrm{j}=1,...,\mathrm{l}$$

Почерговість $\psi(\mathrm{k,l})$ називається розподільником, що відповідає значенням $\mathrm{k}\in \mathrm{K},\ \mathrm{l}\in N$. Так як, розподільник вибирає в кожному такті шифруванні заміну відповідної величини.

Визначаємо правило зашифрування довільного шифру заміни. Якщо $x\in X,\ \mathrm{x}=\mathrm{x}_1...x_i,\ \mathrm{x}\in \mathrm{U},\ \mathrm{i}=1,...,\mathrm{l},\ \mathrm{k}\in \mathrm{K}$ і $\psi(\mathrm{k,l})=\alpha_1^{(k)}$. Тоді $E_k(x)=y$, де $y=y_{1...y_l},\ \mathrm{y}_j\in\varphi_{a_j^{(k)}}(x_j),\ \mathrm{j}=1,...,\mathrm{l}$.

Замість y_j можна вибрати будь-який елемент множини $\varphi_{a_j^{(k)}}(x_j)$, тобто множини $V_{a_j^{(k)}}^{(j)}$. При шифруванні цей вибір можна реалізовувати випадковим чином. Коли відбувається зашифрування, воно не перешкоджає розшифруванню, так як $V_a^{(i)}\cap V_a^{(j)}=\varnothing$ при $i\neq j$.

Класифікація шифрів заміни

Симетричними і асиметричними бувають замінюючі шифри. Симетричне шифрування застосовуються для забезпечення конфіденційності даних. Тут користувачі повинні разом вибрати єдиний математичний алгоритм, який буде застосовуватися для шифрування і розшифрування даних, ключ зашифрування повинен відповідати ключеві розшифрування $k_ç = k_p$. Шифрування асиметричним способом використовує різні, але взаємно доповнюючі один одного ключі $k_ç \neq k_p$ і алгоритми шифрування і розшифрування. Правила зашифрування $E_k(x)$ є багатозначною функцією. Вибір її значень проявляє проблему, яка робить багатозначні функції $E_k(x)$ незручними для застосування. У цьому випадку можна використовувати однозначні функції, що призводить до поділу всіх шифрів заміни на багатозначні і однозначні заміни. Для однозначних шифрів заміни справедлива властивість $\forall \alpha, i\colon \mathrm{V}_a^{(i)} = 1$, а для багатозначних шифрів заміни $\forall \alpha, i\colon \mathrm{V}_a^{(i)} \succ 1$. Шифр який використовують багатозначні заміни можна вказати відомий шифр пропорційної заміни (з'явився в XII столітті), в якому кожній букві ставиться свій еквівалент, число яких пропорційно частоті букви у відкритому тексті. Шифр гамування, на базі якого лежить метод «накладання» ключової послідовності - гами - на відкритий текст, є прикладом шифру однозначної заміни.

Шифри заміни застосовуються для $U \in A^p$ і для деякого $p \in N$. Якщо $p = 1$, тоді, можна сказати про потокові шифри заміни, а якщо $p \succ 1 - 0$ - про блокові шифри заміни. Іншими словами, в потокових шифрах заміни алфавіту множина шифровеличин стикається з алфавітом відкритих повідомлень. Множина блоків відкритого тексту,що ідентична довжині є алфавітом.

Одноалфавітними є шифри якщо $r = 1$ - шифр заміни (шифром заміни або шифром простої заміни). В інших випадках – багатоалфавітний шифром заміни.

На рисунку 1.1 (та наведено в додатку А рис.1) представлено перестановки шифрів, які важливі для класів шифру заміни. Стрілки на даному рисунку, вказують на найбільш важливі підкласи шифрів, а пунктирні стрілки, що ведуть з підкласів шифрів перестановки, означають, що відкритий текст

можна ділити при шифруванні на блоки фіксованої довжини, на кожному з яких виробляється деяка перестановка букв. Різноалфавітні шифри можуть бути потоковими і блоковими. А шифри гамування, що утворюють підклас багатоалфавітних шифрів, можуть відноситься до потокових, а не до блокових шифрів. Крім цього, вони бувають симетричними шифрами.

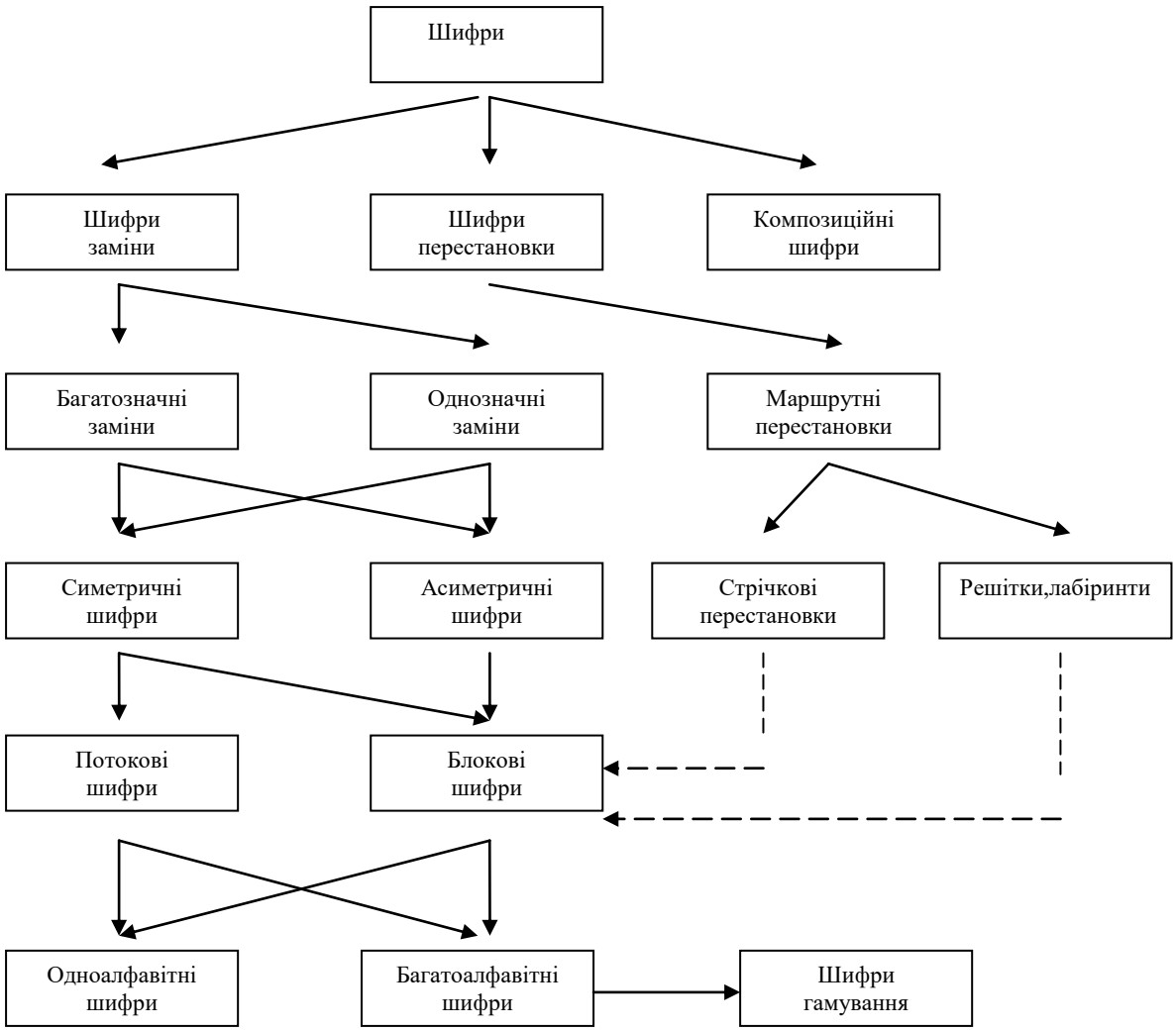


Рисунок 1.1 – Класифікація шифрів

Шифри перестановок.

Шифр перестановки визначається таким чином:

Друге визначення. Нехай $X = Y = A^L$ і нехай $K \subseteq S_L$, де S_L - симетрична складова підстановок множини $\{1, 2, ..., L\}$. Правила шифрування і розшифрування шифру перестановки, для будь-якого ключа k, відкритого тексту $x = (x_1, ..., x_i)$ і зашифрованого тексту $y = (y_1, ..., y_i)$ визначаються формулами:

$$E_k(x) = (x_{k(1)}, ..., x_{k(L)})$$
$$D_k(y) = (y_{k^{-1}(1)}, ..., y_{k^{-1}(L)})$$

де k^{-1} підстановка, зворотна до k. Через такі правила можна сказати що визначення ключ шифру є перестановка номерів символів відкритого тексту. Значні незручності у використанні шифру викликає зв'язаність ключа від довжини тексту. Для зашифрування тексту будь-якої довжини запропоновано ряд приватних шифрів перестановок. Наведемо наприклад, маршрутної перестановки, заснованої на деякій геометричній фігурі. Тут відрізок відкритого тексту записується у фігуру з іншими траєкторіями. Послідовність, при виписуванні тексту на інших траєкторіях називається шифруванням. До прикладу можна записувати повідомлення в прямокутну таблицю, вибравши такий маршрут: ми будемо пересуватися по горизонталі, починаючи з лівого нижнього кута, по черзі справа наліво і зліва направо. Можна по іншому маршруту записувати повідомлення наприклад, по вертикалях, починаючи з нижнього правого кута і просуваючись по черзі знизу вгору і зверху вниз.

Надійність шифрів.

Криптоаналітика є важливою для розкриття на основі надійності або стійкості шифрів. Маючи різні рівні інтелектуального та обчислювального потенціалу, шифросистема може служити об'єктом нападу зловмисника. Головна мета криптоаналітики полягає в отриманні конфіденційної інформації і застосування секретного ключа, за допомогою якого він може розкривати інші криптограми. Дана система може бути надійно захищеною від одних загроз і

опинитися слабкою по відношенню до інших. Криптоатака - спроби зловмисника отримати зашифровану інформацію.

Існують такі види криптоатак:

Атака на основі шифротексту: криптоаналітик визначає хоча б одне з повідомлень $x_i, i = 1,...,m$ (або відповідний ключ k_i), виходячи з необхідного числа m криптограм і має доступ до шифротексту $y_1 = E_{k_1}(x_1),..., y_m = E_{k_m}(x_m)$, які відповідають невідомим відкритим текстам різних повідомлень. У таких випадках можливий збіг ключів: $k_1 = ... = k_m$ чи збіг відкритих текстів $x_1 = ... = x_m$

Атака на основі відомого відкритого тексту: криптоаналітик визначає відкритий текст ще однієї криптограми $y_1 = E_{k_1}(x_1),..., y_m = E_{k_m}(x_m)$ зашифрований, на тому ж ключі при цьому він має доступ до пар $(x_1, y_1),...,(x_m, y_m)$, що відповідають їм шифрованим текстом. Потрібно визначити ключ k_i для хоча б однієї з пар.

Атака на основі обраного відкритого тексту: дана атака відрізняється від попередніх. Тут криптоаналітик має можливість вибору відкритих текстів $x_1 = ... = x_m$ і має доступ до шифратора передавальної сторони, або до систем розпізнавання «свій-чужий».

Атака на основі обраного шифротексту: дана атака відрізняється від інших тим, що криптоаналітик має можливість вибору шифротексту $y_1 = ... = y_m$ і криптоаналітик має доступ до шифратора приймаючої сторони.

Найнебезпечнішими атаками є атаки на основі вибраних текстів. До таких атак додаються і інші. Шифр, що витримує всі можливі атаки, можна визнати надійним або стійким.

Криптоатаки використовують правила Керкгоффса. Суть даного правила полягає в тому, що при реалізації криптоаналізу можна вважати відомою систему шифрування. Секретність ключа шифрування визначається надійністю шифрування. Цей принцип в криптографії пов’язано з тим, що з часом та чи інша інформація про застосовувану шифросистему стає відомою. Слід

підкреслити, що шифри, використовувані спеціальними службами, всіляко охороняються. Шифри з стійкістю є дуже складною проблемою [10].

1.1.3 Системи шифрування

В даний час активно застосовуються два класи систем шифрування: потокові і блокові системи. Основний критерій такого поділу є - потужність алфавіту, над знаками якого проводиться операція шифрування. Коли кожен знак у повідомлені шифрується окремо, то такий шифр буде потоковим. Відкритий текст перед шифруванням може розбиватися на блоки, що складаються з декількох знаків, то тоді це блокова система шифрування.

Точне значення потужності алфавіту, починаючи з якого шифр слід вважати вже не потоковим, а блоковим, назвати не можна. В даний час вживаються 16 - і 32-розрядні процесори, а перспективна шифрувальна техніка проектується вже на 128-розрядних процесорах. Тому при побудові потокових шифрів можуть бути використані алфавіти потужністю 2^{32} і 2^{64}.

Слід підкреслити, що перехід від потокового до блокового шифрування представляє наступні можливості для збільшення надійності та захисту від атак криптографічних алгоритмів. Всі мови володіють великою інформаційною надмірністю. Ентропія тексту - інтегральна характеристика надмірності. Коли у нас є можливість застосовувати статистичні методи для розкриття шифрів ми можемо використовувати їх для текстів з малою ентропією. З підвищенням потужності алфавіту в «новому алфавіті», ентропія на один знак збільшується. Використання таких закономірностей відкритих текстів при проведенні криптографічного аналізу блокових шифрів ми зустрічаємося з деякими труднощами. Крім цього, аналіз таких шифрів пов’язаний з вивченням перетворень алфавітів великої потужності, збільшення розмірів текстів призводить до нелінійного зростання трудомісткості її рішення.

Ускладненням даного аналізу блокових криптосистем є складність аргументування їх криптографічних якостей і отримання доказових оцінок надійності. У таких ситуаціях, треба розробляти методи діагностики, які

враховують специфіку схем блокового шифрування. Недоліки блокових шифрів - складність реалізації перетворень алфавітів великої потужності. Це пов’язано з ефектом розмноження помилок (так як спотворення в окремому знакові може призвести до спотворення головного блоку),що зменшує експлуатаційні якості шифру. Режим простої заміни пов’язаний з необхідністю застосування аналізу «зі словником». Такі недоліки відсутні в потокових шифрах. В даний час на практиці головним чином застосовують потокові шифри, так як вони забезпечують необхідними максимальними швидкостями шифрування. Це важливо при магістральному шифруванні величезної кількості потоків інформації.

Використання потокових шифрів простої заміни (втрата або спотворення) різних символів шифрованого тексту при поширенні по каналу зв’язку призводить до втрат: всі символи шифротексту, приймаються без спотворень і розшифровуються правильно. Ні від розташування знаків в тексті, ні від їх конкретного виду не залежить алгоритм шифрування. При спотворенні окремих знаків шифрованого тексту багатоалфавітного потоку шифри не розподіляють помилки, але є нестійкими до пропусків знаків шифрованого тексту, через це неправильно розшифровується весь текст. При потоковому шифрування застосовують наявність перешкод у всіх каналах передачі даних і в системах криптографічного захисту,тому доводиться забезпечувати про домовленість порядку застосування перетворень при шифруванні різного роду, тобто, вирішувати проблему синхронізації. За методом викреслювання даної проблеми потік шифросистеми поділяють на синхронні системи і системи з самосинхронізацією.

У синхронних потокових шифросистемах, вибір застосовуваних перетворень однозначно визначається розподільником, а також залежить від номера такту шифрування. Кожен символ шифротексту залежить тільки від відповідного символу відкритого тексту та номера такту шифрування, але не залежить від того, які знаки були зашифровані до або після нього. Коли ми розшифровуємо перетворення, воно не залежить від послідовності прийнятих

символів шифротексту. У такому випадку примноження помилки відсутнє повністю. Використання такої системи може призвести до втрати знака шифротексту і призведе до порушення синхронізації і неможливості розшифрування частини повідомлення. Для цього, синхронні потокові шифросистеми передбачають спеціальні процедури відновлення синхронності роботи. Синхронізацію здійснюють додаванням в передане повідомлення спеціальних маркерів. Зрештою, знак шифротексту, пропущений в процесі передачі, призводить до неправильного розшифрування, і поліпшується тоді, коли буде прийнятий один із маркерів.

Інший спосіб зворотного ініціалізації станів, відбувається в ході роботи шифратора одержувача, шифратора відправника при певній попередньо узгодженій умові. Коли синхронізація приймального і передавального шифраторів порушується внаслідок втрати знака шифротексту, тоді потокові системи з самосинхронізацією можуть виробляти точне розшифрування. В режимі зворотного зв'язку найбільш широко застосовуваним є режим використання шифросистем з самосинхронізацією, при якому даний стан системи залежить від деякого числа N попередніх знаків шифротексту. Втрачений знак в такому режимі впливає на N послідовних станів. Після вибору N правильних послідовних знаків з каналу зв'язку стан шифратора стає ідентичним стану передавального шифратора.

1.2 Криптографія та хаос

Останнє десятиліття відоме надзвичайним інтересом до можливості використання динамічного хаосу для шифрування даних. На концептуальному рівні між хаотичними системами і криптографічними системами є своєрідний взаємозв'язок. Тому в нелінійній динаміці, і в криптографії матеріалізувалося нелінійне перетворення інформації. Таке перетворення детерміноване (наприклад, виконується комп'ютером), з іншої сторони, воно має бути непередбачуваним для зовнішнього спостерігача. Тому, слово «детермінований хаос» цілком «підходить» для криптографії.

На практичному рівні між хаотичними і криптографічними системами є своя схожість. Так, як вище зазначалося в класичних роботах К. Шеннона, можна знайти згадку про хаотичні сигнали. Наприклад можна сказати, що він і не вимовляє слово «хаос» в роботі [11], але він пропонує перемішування, що зберігає міру перетворення, що залежать від аргументу і явно згадує основний механізм утворення хаосу через розтягнення і складання.

«Хороші перемішуючі перетворення часто досягаються шляхом повторення двох простих некомутованих операцій». Він показав, що тісто може бути перемішано наступною послідовністю операцій. Спочатку воно розкочується в тонкий шар, потім скочується, потім знову розкочується й скочується і т.д. Якщо добре перемішати, то перетворення функції ускладнюються за рахунок підвищення чутливості всіх змінних. Маленьке збудження в будь-якій з них призводить до значної зміни кінцевого результату.

Проаналізуємо властивості хаотичних систем, які визначають взаємозв'язок хаосу та криптографії.

1.2.1 Хаотична система

Дослідниками відзначено деякі ознаки, при яких спостерігається хаотична поведінка системи [12-13]. Зокрема, необхідною умовою є дві класичні властивості - це топологічна транзитивність і чутливість до початкових умов.

Визначення 1.

Динамічна система (X, f) є хаотичною, якщо релізувати наступні умови:

1) функція $f : X \to x$ топологічно транзитивна на метричній множині $X \subset R^j$. Тобто для будь-яких відкритих множин буває $U,V \subset X$ таке $n \geq 0$, що $f^n(U) \cap V \neq \varnothing$.

2) функція f чутлива до початкових умов. Тобто буває $\delta \succ 0, n \geq 0$ так, що для будь-якого $x \in X$ і його наближення H_x знайдеться $y \in H_x.$, для якого $\left| f^n(x) - f^n(y) \right| \succ \delta$.

Іншими словами, дана система називається хаотичною, якщо всі її траєкторії обмежені, але швидко розходяться в кожній точці фазового простору.

Запити, які задані шифросистемами, схожі на обставини, необхідні для хаотичності динамічних систем. Топологічна транзитивність, потрібна для збереження стану шифросистеми в таких межах, які може допускати носій інформації, і для покриття всього простору станів шифротексту. Чутливість до первинних умов відповідає чутливості до відкритого тексту або / і ключу.

Тому, в теорії хаосу, і в криптографії ми маємо справу з системами, в яких невелика зміна первинних умов призводить до великих змін у всій траєкторії.

1.2.2 Показник Ляпунова

В описі хаотичної системи було введено поняття чутливості до початкових умов. Показник Ляпунова $\lambda(x_0)$ визначається для кожної точки $x_0 \in X$, є мірою чутливості, тобто характеризує швидкість експоненціального розсіювання траєкторій, що знаходяться в наближенні x_0 [14]. Для одновимірної системи

$$\left| f^n(x_0+\varepsilon) - f^n(x_0) \right| = \varepsilon \cdot e^{n\lambda(x_0)} \tag{1.13}$$

де ε - невелике відхилення від початкового стану x_0;

n - число ітерацій (дискретний час).

Тут, λ залежить від первинних умов $\lambda(x_0)$, тому знаходять усереднене значення. Для систем, що зберігають міру λ, залишається постійним для всіх траєкторій. Практично, показник Ляпунова $\lambda(x_0)$ можна обчислити як межу

$$\lambda(x_0) = \lim_{n\to\infty}\lim_{x\to 0}\frac{1}{n}\left|\frac{f^n(x_0+\varepsilon) - f^n(x_0)}{\varepsilon}\right| \tag{1.14}$$

чи

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \log \left| f^n(x_k) \right| = \lim_{n\to\infty} \frac{1}{n} \log \prod_{k=1}^{n} \left| f^n(x_k) \right| \qquad (1.15)$$

Похідна $f^{'}(x_k)$ показує як швидко змінюється функція f даної функцій. Тут для кажного k, по відношенню до зростання аргументу з x_k до x_{k+1}. А межа дорівнює середньому значенню логарифма похідною після n ітерацій і воно являє швидкість розбіжності траєкторій в перебігу дискретного часу n. Якщо $(\lambda \succ 0)$, то воно називається позитивним значенням, який є індикатором хаотичної поведінки системи.

Існує набір $\lambda = \{\lambda_1, ..., \lambda_d\}$ і більш складних поведінок, які якісно не відрізняється від одновимірного випадку для d - мірних систем.

В криптографії, показник Ляпунова є мірою криптографічної ефективності системи. Чим більше λ, тим менше ітерацій потрібно для досягнення даного ступеня розпилення і перемішування інформації.

1.2.3 Ергодичність

Нехай динамічна система $S = (X, f)$ має f □ інваріантну міру $\mu, \mu(X) \prec \infty$ тобто $\forall A \in \sigma(X)$, $\mu(A) = \mu(f^{-1}(A))$, де $\sigma(X)$ є □ σ - алгебра вимірних підмножин X А □ f - інваріантна міра еквівалентна мірі Лебега з функцією щільності розподілу $g(x)$, обмеженою позитивними константами g_1 і g_2: які $0 \prec g_1 \prec g(x) \prec g_2$ де, $\forall A \in \sigma(X)$, $\mu(A) = \int_A g(x)dx$. Коли g_1 близько до g_2, то міра μ близька до рівномірного закону розподілу.

Ергодичною є динамічна система коли існують тільки тривіальні інваріантні множини, тобто для будь-якої вимірної множини, A, f – інваріантною відносно запобіжної міри μ, маємо $\mu(A) = 0$, або $\mu(X / A) = 0$ [15].

Ергодичність - простір X не може бути розділений f - інваріантні нетривіальні і непересічні підмножини. В криптографії ергодичність забезпечує

максимальну стійкість проти криптоаналізу методом перебору, в такому випадку, криптоаналітик повинен вести пошук по всьому простору станів X і не може обмежуватися деякою «передбачуваною» підмножиною.

1.2.4 Перемішування

Перемішувальною системою називається динамічна система, що виконує умову вказану нижче у формулі (1.16):

$$\forall C,\ \mathrm{P} \in \sigma(\mathrm{X}),\ \lim_{n\to\infty}\left(\frac{\mu(f^{-n}(C)\cap P}{\mu(P)} \right) = \frac{\mu(C)}{\mu(X)} \qquad (1.16)$$

Якщо $\mu(X)=1$ (міра μ -імовірнісна), то

$$\lim_{n\to\infty}(\mu(f^{-n}(C)\cap P)) = \mu(C)\mu(P) \qquad (1.17)$$

Перемішувальна властивість динамічної системи означає, що будь-яка множина первинних умов ненульової міри, в кінцевому рахунку, в процесі розвитку системи буде розподілено через весь фазовий простір. Якщо уявити собі безліч відкритих текстів як початкову область у фазовому просторі відображення, тоді перемішувальна властивість буде позначати «поширення впливу одного символу тексту на множину символів шифротексту». Тому, перемішувальна властивість хаотичних явищ знаходиться в близькому відповідно з властивістю розсіювання криптографічних алгоритмів.

Системи з перемішуючою властивістю, мають такі корисні властивості. Коли μ - довільна міра (нормована і абсолютно безперервна стосовно μ) і $\mu_n = \mu_0(F^{-n}C),$ то $\mu_n(C)\to\mu(C)$ для будь-якого вимірювального C. Це означає, що в динамічних системах, що володіють властивістю перемішування, будь-який незрівноважений розподіл прагне до рівноваги. Це означає що, коли кількість ітерацій прагне до нескінченності, статистичні властивості шифротексту не залежатимуть від статистичних властивостей відкритого тексту.

1.2.5 Самосинхронізація

У попередньому розділі було сказано про проблему синхронізації в потокових системах шифрування. Вони дуже чутливі до пропусків знаків шифрованого тексту, тому в них доводиться стежити за узгодженням порядку застосування перетворень при зашифровані і розшифровані. Шляхом введення в передане повідомлення спеціальних маркерів, що безсумнівно приведе до ускладнення самої системи можна забезпечити дане узгодження. Інше рішення полягає у застосуванні систем з самосинхронізацією. Тут, пропущений знак впливає тільки на кілька послідовних станів. Природно, що хаотичні динамічні системи володіють властивістю самосинхронізації, яка виникає автоматично підстроюванням коливань веденої системи в «унісон» з коливаннями ведучої [16-17]. Якими б не були первинні умови в передавачі, в приймачі шляхом самосинхронізації можна взяти точно такий же сигнал. Таким чином, використання заданої властивості динамічного хаосу в традиційних криптографічних схемах допоможе спростити криптографічну процедуру.

1.2.6 Арифметика із плаваючою комою

Використання хаотичної динаміки в системах шифрування може дати останнім нову якість. Така криптографія є цільночисельною. І повідомлення, і гамма (якщо йдеться про шифри гамування), з якою воно складається по модулю або за операцією XOR, яка є послідовностями символів з обмеженим алфавітом, наприклад, послідовностями нулів та одиниць. Хаотичні сигнали бувають принципово безперервними. Реалізація хаотичних джерел на цифрових процесорах або комп'ютерах формально змінює їх в клас дискретних сигналів (як за часом, так і по амплітуді), але у них є своя аналогова природа, яка формує сильні залежності від реалізації обчислювального алгоритму: наприклад, реалізація передавача на цифровому сигнальному процесорі (DSP), а приймача на ЕОМ зі спеціальною довгою арифметикою дадуть дві різні системи, що виробляють різноманітні сигнали, навіть стартуючи з однакових первинних

умов. Якщо в приймачі і передавачі однакова арифметика, то генерувальні ними гамми будуть повністю збігатися.

Арифметика із плаваючою комою обіцяє нові властивості. По-перше, це практично безперервний простір положень систем, обмежене лише реалізацією арифметики. По-друге, застосування хаотичної динаміки надає можливість організації нових криптографічних алгоритмів, які застосовуються для напрацювання з теорії систем зв'язку з застосуванням хаосу. Замість підсумовування повідомлення і гамми по модулю, використовуваного в криптографічних алгоритмах, коли максимальні амплітуди повідомлення і гамми рівні, можна застосувати підсумовування, при якому амплітуда хаотичного сигналу сильно перевершує від амплітуди повідомлення. Коли в звичайних системах зв'язку шум погіршує якість прийому, то при підсумовуванні хаотичного сигналу з інформаційним обставина зворотня: чим більше хаосу, тим краща якість хаотичної синхронізації і краща якість прийнятого сигналу.

1.2.7 Вибір хаотичного відображення

У Таблиці 1.1 узагальнюються подібності та відмінності між криптографічними алгоритмами і хаотичними відображеннями.

Таблиця 1.1 – Характеристики алгоритмів

Хаотичні системи	Криптографічні алгоритми
нелінійні перетворення фазового простору: множина дійсних чисел	нелінійні перетворення фазового простору: множина цілих чисел
ітерація (безкінечне число ітерацій)	повторення (цикли) (кінцеве число повторень)
первинне положення	відкритий текст
кінцеве положення	шифротекст
первинні умови та параметри	ключ
асимптотична незалежність початкового та кінцевого положень	перемішування (confusion)
чутливість до первинних умов та параметрів	розсіювання (diffusion)

Криптографічні алгоритми та хаотичні відображення володіють такими властивостями: чутливість до параметрів і первинних умов, нестійкі періодичні орбіти з довгими періодами і випадково-подібна поведінка. Циклічність, застосовувана при кодуванні в криптографічних алгоритмах, призводить до бажаних властивостей розсіювання і перемішування. Ітерації хаотичного відображення розсіюють початкову область на весь фазовий простір. Ключ алгоритму кодування представляється з параметром хаотичного відображення.

Але з точки зору акцентів і об'єктів вивчення, між криптографією і теорією хаосу бувають такі фундаментальні відмінності:

1) Коли теорія хаосу цікавиться асимптотичною поведінкою системи $(n \to \infty)$, криптографія вивчає ефект кінцевого числа ітераційних перетворень

$(n \prec \infty)$.

2) Класичні хаотичні системи мають дробову розмірність, яка представлена деяким об'єктом (множиною) фазового простору. В даній науці вивчення шифрування, намагаються використовувати всі необхідні комбінації незалежних змінних (що робить систему максимально непередбачуваною) і працюють з просторами з цілими розмірностями.

3) У криптографії аналізуються системи з кінцевим числом станів, а простір станів хаотичної системи визначено на нескінченній множині безперервних або дискретних значень.

4) Криптографічна безпека не володіє аналогом в теорії хаосу (наприклад, у класичній криптографії таким поняттям може служити теорія складності обчислень) та криптографічна безпека хаотичних алгоритмів кодування перевіряється тільки за допомогою криптографічних інструментів.

До таких інструментів належить набір тестів, рекомендованих Національним Інститутом Стандартів і Технологій США, для перевірки якості генераторів, вважають псевдовипадковими.

Монобітовий тест

У послідовності має бути приблизно однакова кількість одиниць і нулів. Частотний тест - рівномірна (перевіряється за допомогою розподілу χ^2) щільність розподілу значень m-бітових блоків (часто $m=4$).

Тест пробігів

Пробігом називається рядок, що складається тільки з нулів або тільки з одиниць (0, 1; 00, 11; 000, 111, ...). Серед усіх пробігів половина повинна мати довжину один біт, одна чверть - довжину два біти, одна восьма - довжину три біта, тоді довжини пробігів відповідає випадковій послідовності.

В якості системи кодування важливо керуватися деякими додатковими критеріями, які необхідні при виборі хаотичного відображення. Кращий алгоритм шифрування поширює вплив одного символу відкритого тексту на множину символів шифротексту. І це поширення впливає на один символ ключа на множину символів шифротексту. Для цього важливо аналізувати тільки такі перетворення, в яких і параметри, і змінні залучаються до чутливого шляху, тобто найменші зміни в одному з них призводять до значних змін в результатах шифрування. Іншими словами, коли нам необхідно застосувати хаотичні відображення в якості криптографічних алгоритмів, ми повинні використовувати властивість перемішування в просторі параметрів. Це означає, що аналізуються тільки ті відображення, для яких хаос буде стаціонарним при малих збуреннях параметрів. Для забезпечення великої кількості ключів, важливо розглядати ті схеми кодування, в яких спостерігається стійкий хаос для великого (краще для всього можливого) діапазону параметрів.

Хаотичний аттрактор визначається властивістю розсіювання в просторі ключів. Такі алгоритми, сформовані на системах зі слабкою складовою стійкості, можуть мати слабкі ключі. Величезна кількість хаотичних аттракторів є конструктивно нестійкими [18]. Таким чином, нам важливо дотримуватися великої передбачливості при підборі хаотичних відображень. Тому що, стійкий хаос не може зустрічатися в гладких системах. У кусково-лінійних відображеннях розглядається структурно-стійкий хаос.

1.3 Висновки до розділу

Отже, основний перелік вимог для хаотичних алгоритмів шифрування:

- в конструкціях криптографічних схем на хаосі важливо використовувати тільки відображення, в яких хаотичний характер стійкий при малих збуреннях параметрів;
- стійкий хаос повинен розглядатися для великої кількості (краще для всього можливого) діапазону параметрів;
- при відображенні початкового повідомлення в зашифроване, в останньому не повинно бути ніяких структур;
- схема шифрування повинна бути чутливою порівняно відкритого тексту і відносно ключа;
- схема шифрування має бути симетричною порівняно від часу шифрування/розшифрування;
- велика кількість зашифрованого повідомлення не повинна сильно перевищувати обсяг початкового повідомлення;
- важливо щоб схема була простою по своїх конструкціях і повинна володіти високими швидкостями шифрування;
- можливість адаптації схеми кодування до різних типів інформаційних сигналів;
- можливість зміни довжини ключа;
- схема повинна бути стійкою до основних видів криптографічних атак (атака «грубої сили», тобто перебором і атак на базі, відомих шифротекстів).

2 ВИКОРИСТАННЯ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

В даному розділі роглянуто основне поняття хаосу, його властивості та особливості, найвідоміші на сьогоднішній день алгоритми передачі інформації із застосуванням хаосу, а також зразок системи зв'язку з маскуванням інформаційного сигналу псевдовипадковим сигналом схеми Чуа.

2.1 Поняття хаосу

Зростаючі обсяги інформації мобільних систем телекомунікацій постійно потребують збільшення пропускних спроможностей каналів зв'язку. Особливо гостро стоїть проблема розробки радіосистем, що могли б функціонувати із вже існуючими системами мобільних комунікацій в одному і тому самому частотному діапазоні. Можливість спільного існування різних систем в межах одного частотного ресурсу потребує суттєвої відмінності застосованих сигналів у різних системах. Якщо традиційні системи використовують модульовані гармонічні коливання, то має сенс у нових системах використовувати хаотичні сигнали.

Хаотичні коливання утворюються в хаотичних нелінійних нестійких динамічних системах, тобто вони є результатом еволюції поведінки цих систем. Форма сигналів хаос-генераторів носить випадковий характер, але такі сигнали мають важливі відмінності від шумових сигналів, що торкаються як способу їх отримання так і статистичних характеристик. Найбільш повно відмінність хаотичних і випадкових сигналів пояснюється за допомогою фазових траєкторій. Для випадкових процесів фазові траєкторії є випадковими, непередбачуваними та не відтворюваними повторно, тобто під час запуску шумоподібного генератора за однакових початкових умов отримуються різні фазові траєкторії. Хаотичні коливання, незважаючи на складність форми та її зміну у часі є відтворюваними, за умови відтворення початкових умов збудження [19].

Приваблива особливість хаотичних систем полягає у можливості управління хаотичними режимами шляхом малих змін параметрів системи. Структура виду коливань, за умови невеликої зміни керуючого параметра, може змінитися у незначній мірі, але це буде вже інша хаотична мода і факт цієї зміни може бути надійно зафіксований. Якщо в системі є декілька змінних параметрів, то варіювання кожним з них окремо або одночасно буде приводити до зміни типу хаотичної моди. Тому введення інформації в хаотичний сигнал може здійснюватися за допомогою зміни параметра (параметрів), а виділення інформації в приймачі здійснюється за рахунок вибору параметрів приймача і забезпечення хаотичної синхронізації.

Що ж таке хаос? Говорячи «хаос», ми, звичайно, маємо на увазі повна відсутність порядку, абсолютну невпорядкованість і випадковість. З математичної точки зору, хаос і порядок - поняття не взаємовиключні. Теорія хаосу - досить молода математична область, створення якої прирівнюють за значимістю відкриттів XX століття до створення квантової механіки. Хаос трапляється в нелінійних динамічних системах. Інакше кажучи, будь-який процес, який протікає з часом, може бути хаотичним.

Щоб розібратися, що таке хаос, спочатку звернемося до систем, що такою рисою не наділені. Детерміновані системи не допускають ніяких випадковостей: значення на виході повністю визначено значеннями на вході. Таким чином, зміна початкових умов викликає пропорційну зміну результату.

Великий внесок в теорію хаосу вніс метеоролог Едвард Лоренц. У шістдесятих роках минулого століття цей американець працював над комп’ютерною програмою, що моделює рух повітряних мас в атмосфері Землі. Всі ми знаємо, що комп’ютер (всупереч розхожим чуткам) є строго детермінованою системою, і це створює відомий принцип «garbage in garbage out». Модель Лоренца виявилася надчутлива до початкових умов. Найменше розходження у вхідних даних приводило до сильного розбіжності результатів із часом. Ця залежність від початкових умов і була названа хаосом.

Динамічний хаос (ДХ) складний, невпорядкований рух нелінійних систем, що виникає при відсутності будь-яких випадкових збурень. Для реалізації нетрадиційних алгоритмів запису, зберігання, обробки і передачі інформації, що використовують властивості хаотичної динаміки систем, необхідні генератори хаосу (ГХ) пристрої, що перетворюють енергію, взяту від деякого зовнішнього джерела, в енергію хаотичних коливань.

Основна властивість ДХ - висока чутливість до початкових умов. Динамічний хаос володіє багатьма властивостями випадкових процесів:

1. Суцільний спектр потужності (ця властивість може бути використана для розрізнення хаотичної динаміки від багатоперіодичного руху);

2. Експоненціальний спад кореляційної функції;

3. «Горизонт прогнозу» - непередбачуваність на великих інтервалах.

Причини, що визначають привабливість хаосу для використання в системах передачі інформації:

1. Можливість отримання складних коливань за допомогою простих моделей і, відповідно, пристроїв;

2. Можливість реалізації великої кількості моделей хаотичної динаміки в одному пристрої (заснована на високій чутливості до початкових умов);

3. Можливість управління хаотичними режимами за допомогою малих керуючих впливів (малих змін параметрів системи). Цей пункт має як «+», так і «-». Плюс - можливість керуючого сигналу суттєво нижча за потужність модулюючого. Мінус - висока чутливість;

4. Висока інформаційна ємність;

5.Велике число можливих методів модуляції (введення інформаційного сигналу в сигнал хаотичний). Для регулярного сигналу три види модуляції (амплітуда, частота, фаза), а для хаотичного ще й:

5.1. модуляція параметрів;

5.2. нелінійне підмішування інформаційного сигналу до хаотичного;

5.3. корекція траєкторій хаотичної системи малими збудженнями;

5.4. Використання тонкої структури аттрактора;

6. Можливість збільшення швидкості модуляції в порівнянні з швидкістю модуляції регулярних сигналів;

7. Можливість самосинхронізації передавача і приймача;

8. Можливість розробки та використання нетрадиційних методів мультиплексування;

9. Можливість підвищення ступеня конфіденційності зв'язку. Деякі методи забезпечення конфіденційності зв'язку:

9.1. Хаотичне маскування;

9.2. Перемикання хаотичних режимів;

9.3. Нелінійне підмішування;

9.4. Використання фазового автопідстроювання частоти;

9.5. Інверсні схеми;

9.6. Слабкі місця хаотичних методів передачі інформації:

1. Висока чутливість до спотворень в каналі зв'язку; 2. Висока чутливість до шумів; 3. Висока чутливість до неповної ідентичності параметрів приймача і передавача [20].

2.2 Алгоритми передачі інформації, засновані на використанні ефектів хаотичної динаміки

Розглянемо відомі на сьогоднішній день алгоритми передачі інформації із застосуванням хаосу (та наведено в додатку А рис.2). При хаотичному маскуванні (рисунок 2.1) інформаційний сигнал $s(t)$ підсумовується з вихідним сигналом $y(t)$ генератора хаосу (ведуча система). Результуючий сигнал $s(t)+y(t)$ передається в канал. Ведена система (приймач) являє собою узгоджений з даними генератором хаосу нелінійний фільтр і володіє тією властивістю, що при надходженні на неї сигналу від цього генератора сигнали на її вході і виході збігаються.

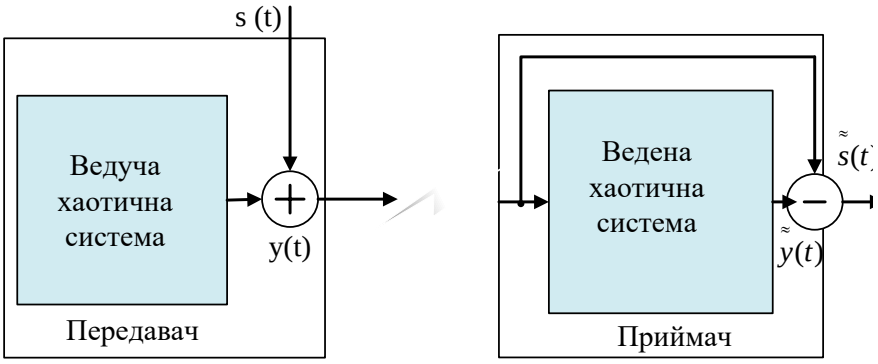


Рисунок 2.1 – Хаотичне маскування

Якщо вхідний сигнал незначно збурений по відношенню до сигналу на виході генератора хаосу, то це збурення зменшується при проходженні через ведену систему. Ця обставина використовується в розглянутій схемі: за оцінку інформаційного сигналу приймається різниця сигналів на вході і виході веденої системи. Схема працездатна, якщо потужність інформаційного сигналу набагато менше, ніж потужність сигналу в каналі зв'язку. Це призводить до низького відношенню сигнал/шум на виході приймача.

При перемиканні хаотичних режимів (рисунок 2.2), (та наведено в додатку А рис.3). бінарний інформаційний сигнал $s(t)$ кодується за допомогою передачі хаотичного сигналу одного типу, коли передається «1», і хаотичним сигналом іншого типу, коли передається «0». Ці хаотичні сигнали вибираються таким чином, щоб мати подібні статистичні і спектральні властивості. Перемикання хаотичних режимів забезпечує можливість достатньо простої конфігурації приймача, проте при перемиканні хаотичного режиму потрібен якийсь час для встановлення синхронізації, тому швидкість передачі даних відносно невелика.

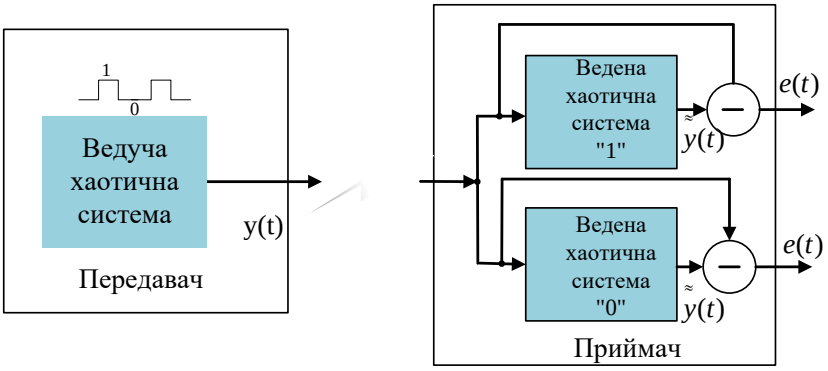


Рисунок 2.2 – Перемикання хаотичних режимів

При нелінійному підмішуванні інформаційний сигнал безпосередньо бере участь у формуванні складної хаотичної поведінки ведучої системи. Таке введення інформації не можна назвати ні адитивним накладенням, ні звичайною модуляцією. У ведучій системі інформаційний сигнал $s(t)$ підмішується до власного сигналу системи $y(t)$ у. Наприклад, це може бути зроблено шляхом введення його в кільце зворотного зв'язку генератора хаосу, що представляє собою послідовне з'єднання фільтрів нижніх частот першого (R_1C_1) і другого (R_2LC_2) порядків і нелінійного елемента з амплітудною характеристикою F (z) (рисунок 2.3), (та наведено в додатку А рис.4).

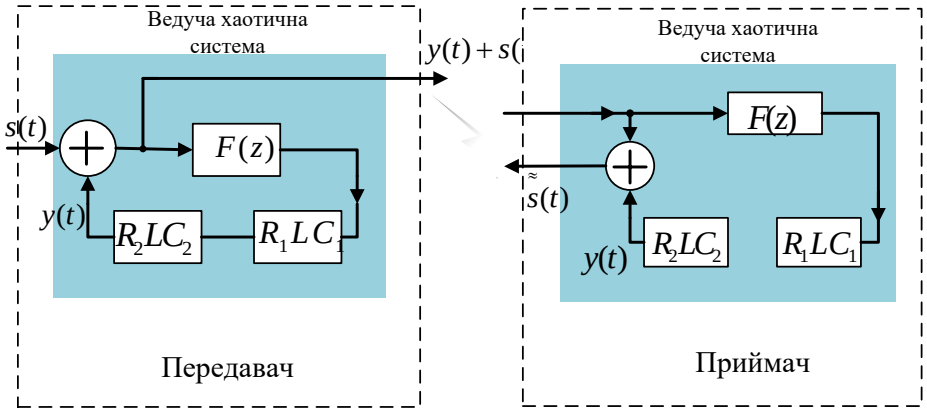


Рисунок 2.3 – Нелінійне підмішування сигналів

Для вилучення інформації в приймачі використовується узгоджений нелінійний фільтр, який здійснює той же тип нелінійного перетворення, що і в передавачі. Далі виробляється віднімання сигналу, що пройшов фільтр, з сигналу, що надійшов на вхід фільтра (ведена система). Слід зазначити, що в системі з нелінійним підмішуванням при повністю узгодженому фільтрі інформаційний сигнал на виході приймача витягується точно.

При рознесенні в просторі окремих частин єдиного хаотичного генератора між «ведучою» і «веденою» системами використовуються два канали зв'язку (рисунок 2.4), (та наведено в додатку А рис.5).

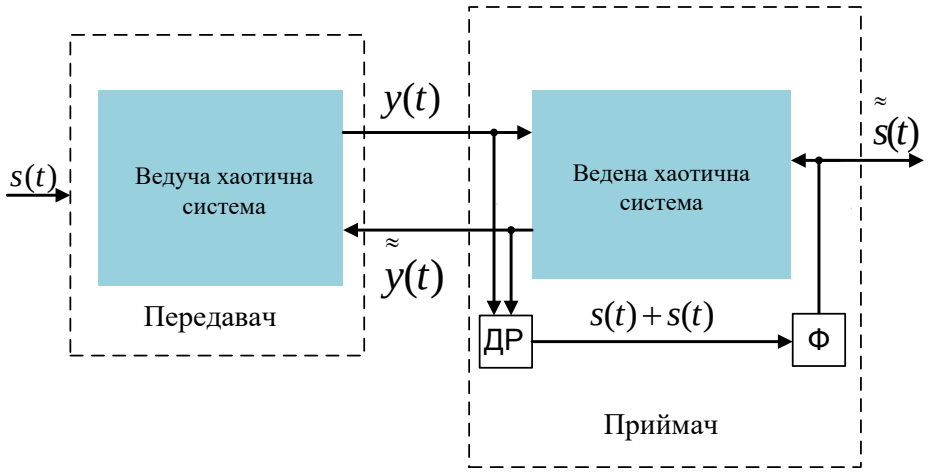


Рисунок 2.4 – Рознесення сигналів

Принцип передачі інформації полягає в наступному: сигнал $s(t)$ на вході провідної системи збурює її режим, який, однак, залишається хаотичним. За розбіжність сигналів $y_1(t)$ і $y_2(t)$ в прямому і зворотному каналах, на приймальному кінці тракту працює система, що відновлює інформацію. Перевагою зазначеного методу реалізації системи зв'язку є не настільки помітна, як у трьох попередніх, чутливість до розстройки параметрів приймача і передавача. Але потрібно два канали зв'язку, що не завжди прийнятно на практиці.

При побудові систем з розширенням спектра структура каналоутворюючої апаратури залишається традиційною для даного класу систем зв’язку. Але генератор псевдовипадкової послідовності на передавальній стороні замінюється генератором бінарного хаотичного сигналу, і аналогічний генератор поміщається в приймач. Щоб ці генератори працювали синхронно, застосовується схема стеження за затримкою, а на початку сеансу зв’язку в канал передаються початкові умови для генерації. У разі втрати синхронізації відновити стеження можна тільки шляхом одночасного перезапуску генераторів хаосу в приймачі і передавачі. Перевагою такої CDMA-системи перед звичайною є практично необмежена ємність ансамблю послідовностей, що розширюють спектр. Недолік схеми складність пошукової процедури при втраті синхронізації [21].

2.3 Генератори хаосу малого степеня інтеграції

В наш час інтенсивно досліджуються системи зв’язку, в основу роботи яких покладені властивості детермінованого хаосу. Генератори хаосу в переважній більшості прості по конструкції. Це є наслідком вимоги відтворюваності режимів роботи та їх характеристик. На рисунку 2.5 (та наведено в додатку А рис.6) приведена схема генератора Чуа. Вона включає в себе чотири стандартних елемента (R, C_1, C_2, L) і нелінійне опір (діод Чуа) з кусково-лінійною характеристикою. На сьогоднішній день відомо кілька схемотехнік діода Чуа. Всі вони представляють собою комбінації декількох стандартних елементів з операційними підсилювачами та / або діодами. Реалізація такого роду пристроїв на ІС малому степені інтеграції передбачає індивідуальний підбір однакових елементів в передавачі і приймачі з максимально можливою точністю.

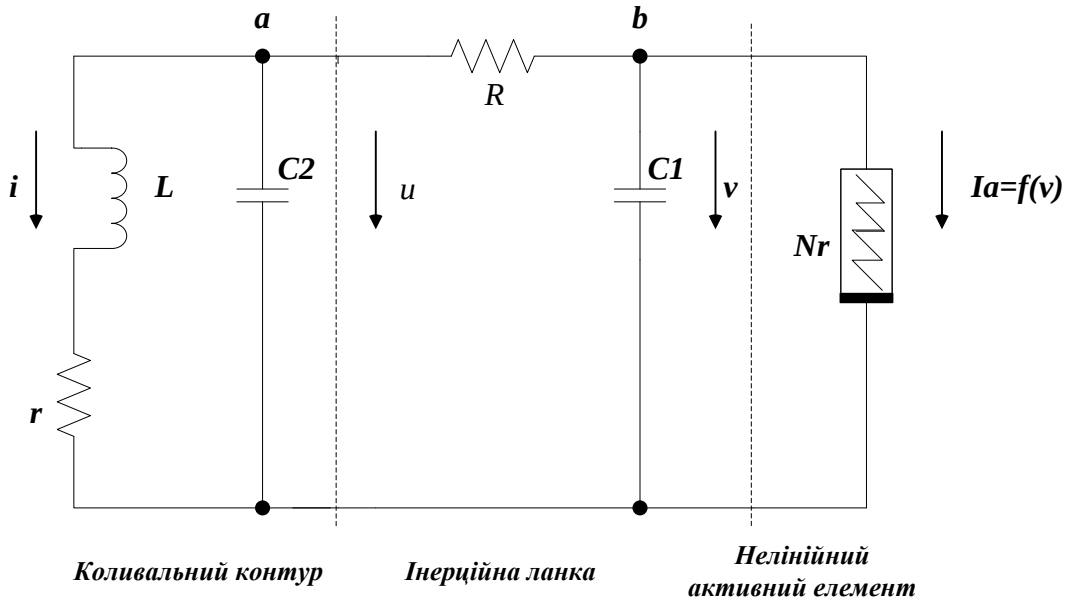


Рисунок 2.5 – Схема генератора Чуа

Для ілюстрації обмежених можливостей даного підходу розглянемо проведений експеримент з передачі суміші інформаційного сигналу з хаотичним через радіоканал. Приймально-передавальний тракт був стандартним, операції підмішування хаотичного сигналу до інформаційного та відновлення інформаційного сигналу з суміші з хаотичним реалізовувалися за допомогою двох хаотичних модулів.

Базовим елементом приймально-передавальних трактів динамічних систем є так званий «діод Чуа», тобто радіокомпонент, який має суттєві нелінійні властивості. Його наявність є необхідною умовою для реалізації у вказаних системах хаотичних коливань. В подальшому при аналізі передавання, приймання та обробки інформації в хаотичних системах зв’язку в більшості робіт поведінка нелінійних елементів описується в основному аналітично.Чисельне моделювання і, особливо, саме аналіз експериментальних результатів роботи нелінійних елементів дають можливість повноцінно використовувати всі переваги детермінованого хаосу при практичній реалізації сучасних захищених систем зв’язку.

Розглянемо більш детально роботу схеми Чуа, яка є однією із найпростіших систем з хаотичною поведінкою і представляє собою автоколивальну систему з 1,5 степенями свободи.

Схема складається з коливного контуру з втратами rLC_2, інерційної ланки RC_1 і активного нелінійного елемента, зображеного на схемі в вигляді нелінійної провідності (рисунок 2.5).

Генеруючий резонансний коливний контур rLC_2 зв'язаний з активним нелінійним елементом через інерційну ланку RC_1. Поведінка системи визначається впливом нелінійного елемента, що відіграє роль джерела живлення системи. Нагадаємо, що присутність нелінійності є необхідною, але недостатньою умовою для виникнення хаосу в системі.

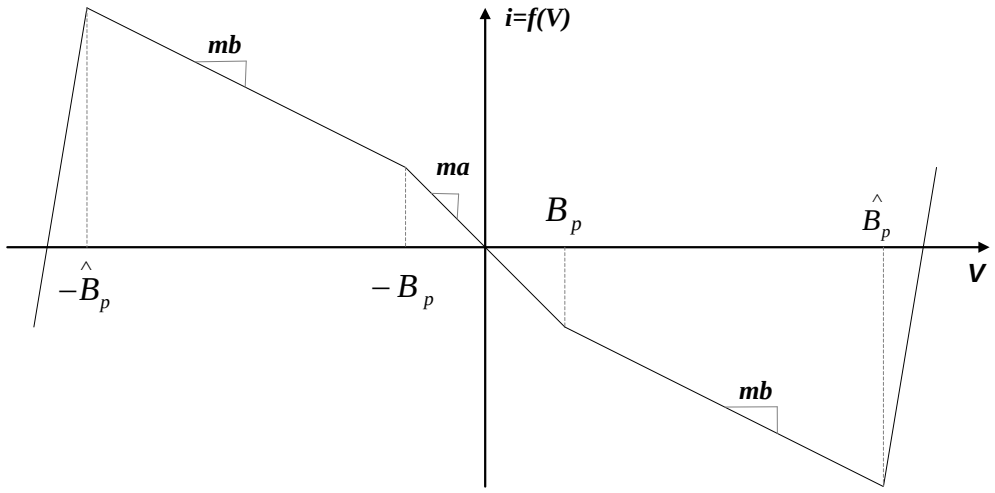


Рисунок 2.6– Вольт-амперна характеристика нелінійного елемента

Обмежений характер хаотичних траєкторій обумовлений розсіюванням енергії в пасивних елементах R і r, що стримує її зростання в коливному контурі. Проте баланс енергії виявляється досить нестійким, неперервно змінюється в часі і ніколи не повторюється як періодичне явище. Візьмемо як складові компоненти вектора стану системи струм i в контурі, напругу u на ємності C_2 контура rLC_2 і напругу v на нелінійному елементі. Згідно з першим і другим законів Кірхгофа запишемо систему трьох диференціальних рівнянь:

$$\left\{\begin{array}{l} L\dfrac{d_i}{dt} = -r_i - u \\ C_2\dfrac{du}{dt} = i + \dfrac{v-u}{R} \\ C_1 = \dfrac{u-v}{R} - f(v), \end{array}\right\} \qquad (2.1)$$

де f(v) – кусково-лінійна характеристика нелінійного елемента;

$$f(v) = m_b v + 0,5(m_b - m_a)\left[\left|v + B_p\right| - \left|v - B_p\right|\right], \qquad (2.2)$$

тут m_a, m_b - розміри крутизни лінійних ділянок;

$+B_p, -B_p$ – точки перегину нелінійної характеристики (рисунок 2.6), (та наведено в додатку А рис.7).

Перше рівняння представляє суму падіння напруги при круговому обході резонансного коливного контура, а друге і третє дають відповідно суму струмів для вузлових точок a і b схеми, представленої на рисунок 2.5. Проведемо нормування змінних i, u, v в системі відносно напруги B_p:

$$x = v / B_{p,y} = u / B_{p,z} = R_i / B_p \qquad (2.3)$$

і перейдемо до безрозмірного часу $\underline{t} = t / R_c$.

В безрозмірних величинах система рівнянь (1), що описує схему Чуа, приймає такий вигляд:

$$\left\{\begin{array}{l} dx / d\underline{t} = \alpha\left[y - x - f(x)\right]; \\ dy / d\underline{t} = x - y + z; \\ dz / d\underline{t} = -By + (T / T_k)z, \end{array}\right. \qquad (2.4)$$

де $\alpha = C_2 / C_1$, $\beta = T / \tau$, T=RC (міра інерційності RC кола); $T_k = L / r$, де T=RC.

З врахуванням нормування напруги $v = x \cdot B_p$ можемо замість (2.4) записати безрозмірну характеристику активного елемента у вигляді:

$$f(x) = bx + 0,5(a-b)\left[|x+1| - |x-1|\right], \qquad (2.5)$$

де коефіцієнти $a = Rm_a$, b=Rm_b – також безрозмірні величини. Щоб спростити аналіз схеми, знехтуємо доданком $(T/T_k)_z$ в третьому рівнянні (4). Це значить, що ми нехтуємо втратами в rLC_2 контурі, приймаючи, що r=0. Тоді при вибраних коефіцієнтах a, b характеристики (5) реалізація тих чи інших процесів у схемі Чуа визначається значеннями її двох основних параметрів. Роль першого параметра відіграє відношення ємностей $\alpha = C/C_1$, а другого – відношення постійних часу $\tau = L/R$. Постійна $T = RC$ є мірою інерційності RC кола, а постійна часу $\tau = L/R$ характеризує інерційність ланки, що складається з елементів L і R [22].

2.4 Криптосистема за схемою Чуа

Розглянемо найпростіший алгоритм передавання інформації із застосуванням генераторів хаосу [23]. Інформаційний сигнал $s_1(t)$ підсумовують з вихідним сигналом $y_1(t)$ генератора хаосу в передавачі (рис. 2.7), (та наведено в додатку А рис.8). Сумарний сигнал $s_1(t) + y_1(t)$ передають у канал зв'язку.

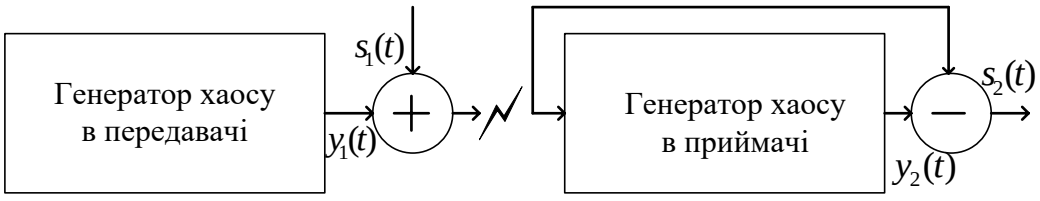


Рисунок 2.7- Схема маскування хаотичним сигналом

У приймачі генератор хаосу узгоджений (синхронізований) з генератором передавача. Тому сигнали хаосу $y_1(t)$ та $y_2(t)$ збігаються. Тоді вихідний сигнал приймача $s_2(t) = (s_1(t) + y_1(t)) - y_2(t) = s_1(t)$ збігається з вхідним сигналом передавача. Якщо енергія інформаційного сигналу значно менша від енергії сигналу генератора хаосу, то на фоні псевдовипадкового сигналу корисний сигнал непомітний. Отже, така система зв'язку приховує інформаційний сигнал, тобто є системою криптозв'язку. Передавач і приймач криптосистеми містять схеми Чуа. Схема передавача і приймача на вхідній мові Micro-Cap показана на рисунку 2.8.

Вихідні сигнали схем Чуа – це напруги на діодах Чуа. У передавачі напруга V_2 підсумовується з напругою V_1 синусоїдного джерела частотою 5 кГц, яка імітує інформаційне повідомлення. Номінали елементів схем Чуа в приймачі та передавачі збігаються. Але навіть за цієї умови вихідні сигнали двох схем з часом помітно відрізняються внаслідок накопичення похибок числового інтегрування. Це є проявом особливості дивного аттрактора. Тому для правильного відтворення інформаційного сигналу в приймачі необхідно час від часу вирівнювати значення змінних стану, тобто значення напруг на конденсаторах і струмів у індуктивностях [24]. Схема Чуа в приймачі відрізняється від схеми у передавачі елементами синхронізації R_2, R_3 (передавача). Синхронізація генераторів хаосу забезпечена періодичним передаванням вектора стану схеми Чуа від передавача до приймача.

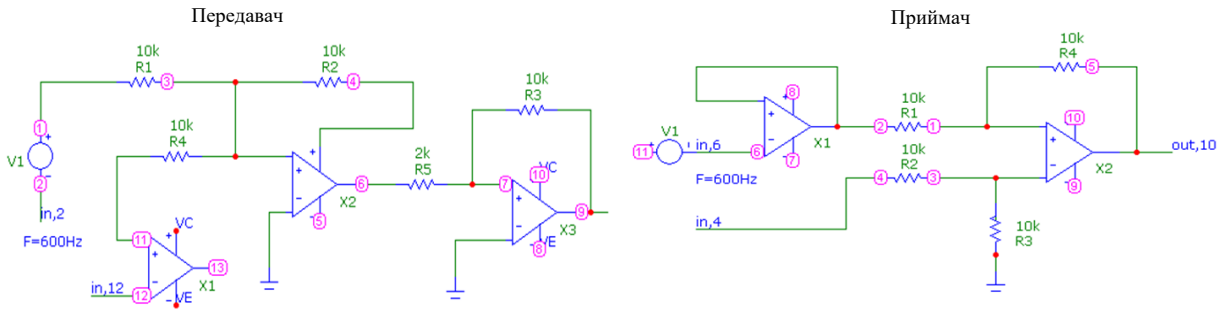


Рисунок 2.8 - Схема криптосистеми

Джерело імпульсів синхронізації задає інтервали синхронізації. Майже постійно V_{10}=0, лише впродовж 0,1 мс на початку кожних 25 мс V_{10}(10)=1. Керовані джерела повторюють змінні стану схеми передавача. Опори R_2, R_3 змінюють значення від 10 кОм до 0 залежно від значення напруги V.Завдяки цьому впродовж 0,1 мс кожні 25 мс у схемі приймача примусово задаються струм індуктивності та напруги ємностей, які збігаються з відповідними у схемі передавача. На суматорі X_2 віднімається прийнятий сигнал на виході від сигналу входу.

Часові діаграми сигналів криптосистеми, зображені на рисунку 2.9 : вихід схеми генератора Чуа передавача; інформаційний сигнал; вихідний сигнал передавача; вихід схеми генератора Чуа приймача ; інформаційний сигнал відтворений у приймачі [25].

Як бачимо, на виході приймача повністю відтворений інформаційний сигнал.

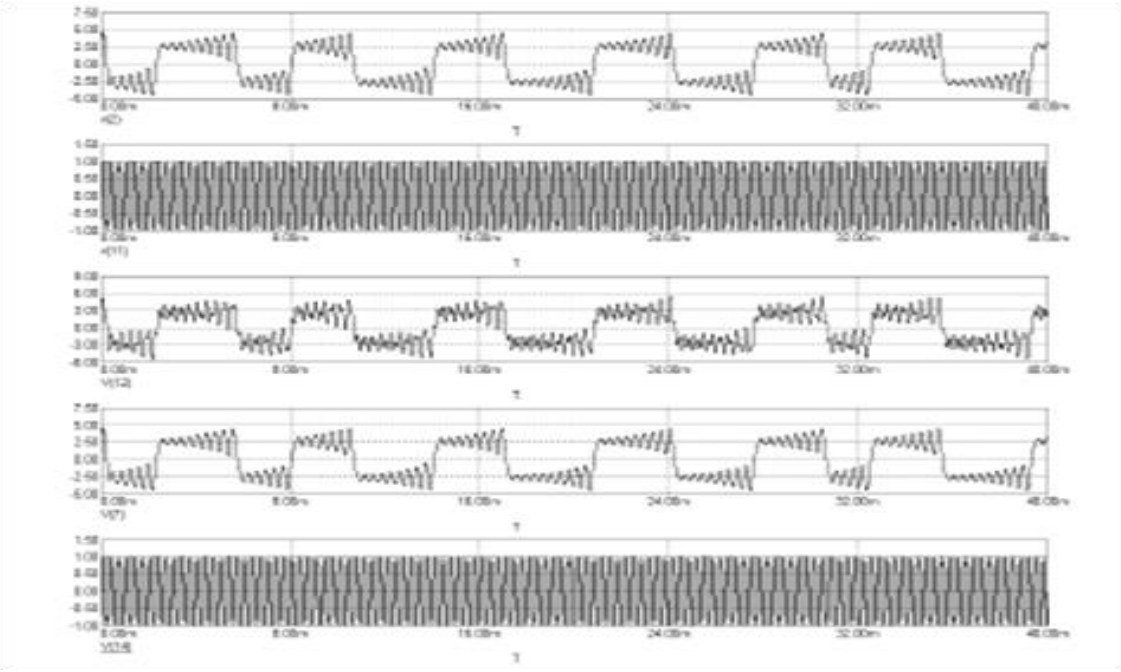


Рисунок 2.9 - Часові діаграми сигналів криптосистеми

2.5 Висновки до розділу

В даному розділі було розглянуто основне поняття хаосу, його властивості та особливості, найвідоміші на сьогоднішній день алгоритми передачі інформації із застосуванням хаосу. Детально описано роботу схеми Чуа, яка є однією із найпростіших систем з хаотичною поведінкою.

Також описано зразок системи зв’язку з маскуванням інформаційного сигналу псевдовипадковим сигналом схеми Чуа. Отже, описаний зразок системи є ілюстрацією принципової можливості системи захисту інформації.

3 РОЗРОБЛЕННЯ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ НА ПРИЛАДІ З ВІД'ЄМНИМ ДИФЕРЕНЦІЙНИМ ОПОРОМ

В даному розділі розрахуємо номінали елементів експериментальної моделі схеми генератора Чуа, розглянемо реалізацію схеми генератора Чуа на схемотехнічних приладах із від'ємним диференційним опором, а також виконаємо комп'ютерне моделювання генератора хаотичних коливань та дослідимо його властивості.

3.1 Розрахунок номіналів елементів електричної схеми генератора Чуа

Аттрактор типу «подвійний виток» з'являється в ланцюзі Чуа при наступних значеннях параметрів:

$C_1 = 1/9$; $C_2 = 1$; $L = 1/7$; $G = 0,7$; $B_p = 1$; $m_0 = -0,5$; $m_1 = -0,8$.

У прикладах моделювання одиниці вимірювання не наводилися для змінних стану v_{c_1}, v_{c_2} і i_L, оскільки просто моделювався набір диференціальних рівнянь. Переписавши рівняння в одиницях СІ, напруги будуть вимірюватися в вольтах (Вт), струми в амперах (А), ємність у Фарадах (Ф), індуктивність в генрі (Гн), опір в омах (Ом); величина обернена опору називається провідністю, вимірюється в Сіменсах (См). Оскільки в електронних ланцюгах легше реалізувати струми порядка міліампер, ніж ампер, то першим кроком є зменшення всіх струмів в 1000 разів, що веде до зменшення всіх ємностей в 1000 разів і збільшенню опорів і індуктивностей в стільки ж разів [26].

Таким чином, при v_{c_1} і v_{c_2}, вимірюваних в вольтах і i_L вимірюваному в міліампер, набір параметрів приймає вигляд:

$C_1 = 1/ 9*10^{-3}$ Ф,

$C_2 = 1*10^{-3}$ Ф,

$L = 1/7*10^{3}$ Гн,

$G = 0,7*10^{-3}$ См.

Нахили кусково-лінійної характеристики резистора складають тепер -0,8 мСм (мА / В) і -0,5 мСм; точки зламу залишаються незмінними при B_p = 1В. Простіше використовувати ємності в нанофарадах і індуктивності в міллігенрі, ніж Фаради і генри. Ефект перемасштабування часу в k раз проявляється в множенні кожної індуктивності і ємності на той же множник k; на величини резисторів зміна масштабу часу не впливає. Зокрема, уповільнення часу в $2*10^4$ разів зменшує C_1, C_2 і L в стільки ж разів. Змінені параметри приймають такий вигляд:

$C_1 = 1/18*10^{-7}$ Ф = 5,56 нФ,

$C_2 = 1,2*10^{-7}$ Ф = 50 нФ,

$L = 1/14*10^{-1}$ Гн = 7,14 мГн,

$G = 0.7*10^{-3}$ См = 0,7 мСм (що відповідає R = 1428 Ом).

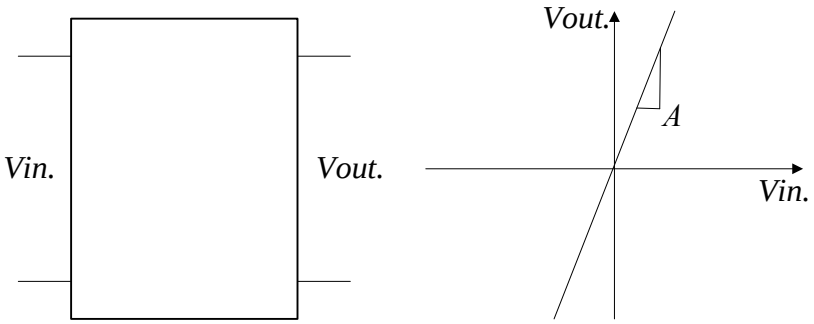
При перемасштабуванні часу точки зламу і нахилу кусково-лінійного резистора NR не змінюються. Виберемо номінали реальних елементів рівними 18 мГн, 10 нФ, 100 нФ і 1800 Ом, близьких до розрахункових. Провівши масштабування струму і часу, ми сконструюєм діод Чуа: нелінійний резистор з вольт-амперними характеристиками. Його важливою властивістю є те, що він володіє двома негативними нахилами m_0 і m_1.

3.2 Реалізація схемотехнічного аналогу приладу з від'ємним диференційним опором на операційних підсилювачах

Існує безліч шляхів для синтезу негативного опору, один з яких полягає в приєднанні трьох позитивних лінійних резисторів до керованого напругою джерела напруги для формування перетворювача негативного опору. Це пристрій привабливий з експериментальної точки зору, оскільки легко здійснюється за допомогою операційного підсилювача (ОП).

Кероване напругою джерело напруги є ідеальним елементом ланцюга, який має два входи і два виходи (рисунок 3.1). Він характеризується двома властивостями: струм на вході дорівнює нулю, а напруга на виході ν_{out} є

функцією різниці потенціалів на вході v_{in}.Найпростіша нетривіальна функціональна залежність між вхідною і вихідною напругами кероване напругою джерело напруги має місце, коли v_{out} лінійно залежить від v_{in}, тобто $v_{out} = Av_{in}$. Це проілюстровано на рисунку 3.1.



а) б)

Рисунок 3.1 – Джерело напруги: графічне позначення (а) і передавальна характеристика (б)

Тепер ми можемо отримати перетворювач негативного опору з двома виводами, під'єднуючи три позитивних резистора до керованого напругою джерело напруги, як показано на рисунку 3.2а.

Припустимо, що кероване напругою джерело напруги на рисунку 3.2а є лінійним, з функцією перетворення напруги $v_{out} = Av_{in}$.

За законом Кірхгофа для струмів у вузлі 1 на рисунку 3.2

$$i = \frac{1}{R_1}(v - v_{out}) \tag{3.1}$$

Напруги в контурі 1-3-0-1 пов'язані співвідношенням

$$v = v_{in} + \left[\frac{R_3}{R_2 + R_3}\right] v_{out} \tag{3.2}$$

Передавальна функція для КНДН задається як

$$v_{out} = Av_{in} \tag{3.3}$$

Отже, з 3.2 і 3.3 $v = \left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] v_{out}$.

Або, що еквівалентно, $v_{out} = \left[\frac{A(R_2 + R_3)}{R_2 + (1+A)R_3} \right] v$.

Підставляючи v_{out} в 3.1, отримуємо $i = \left[\frac{(1-A)R_2R_3}{R_1[R_2] + (1+A)R_3} \right] v$.

При великих A $i \approx -\left[\frac{R_2}{R_1R_3} \right] v$.

Далі, вибираючи $R_1 = R_2$,отримаємо $i \approx -\frac{1}{R_3} v$.

Цей результат графічно представлений на рисунку 3.2 б. Таким чином, підключаючись до вхідних затискачів елемента N_R, ми спостерігаємо опір $-R_3$.

У реальних пристроях є деякий робочий діапазон, в якому можна говорити про відповідність поведінки моделі і реального приладу. Операційний підсилювач - це електронний прилад, який в деякому діапазоні вхідних напруг дає апроксимацію джерела напруги, керованою напругою.

Розглянемо ланцюг, показаний на рисунку 3.3а. Він складається з операційного підсилювача і пов’язаних з ним джерел живлення V^+і V^-.

Напруга, прикладена між неінвертуючим і інвертуючим входами (позначеними "+" і "-"), виробляє різницю потенціалів між виходом і опорним виводом (зазвичай загальна точка джерел живлення).

Цей реальний схемний модуль з ОП має невеликий вхідний струм i_{in}; вважатимемо $i_{in} = 0$.

Коли диференціальна вхідна напруга v_{in} реального ОП досить велика по модулю і негативна, на виході ми маємо практично постійну напругу $-E_{sat}^-$; ця область називається областю від’ємного насичення.

Коли на вході невелика напруга, то вихідна напруга змінюється майже лінійно залежно від вхідного; ця область називаєся лінійною. Коефіцієнт посилення в лінійній області зазвичай перевищує 10^5. Крім того, характеристика стоїть від початку координат на вхідну напругу зміщення v_{os} (вона може бути негативною або позитивною, властивою одному конкрет- ному пристрою), яке зазвичай становить кілька мілівольт. Коли вхідна напруга велика і позитивна, напруга на виході приймає максимальне значення E_{sat}^{+}; ця область називається областю позитивного насичення. Таким чином, функція перетворення постійної напруги для реального ОП добре апроксимується трьохсегментною кусково-лінійною характеристикою, яка показано на рисунку 3.2б.

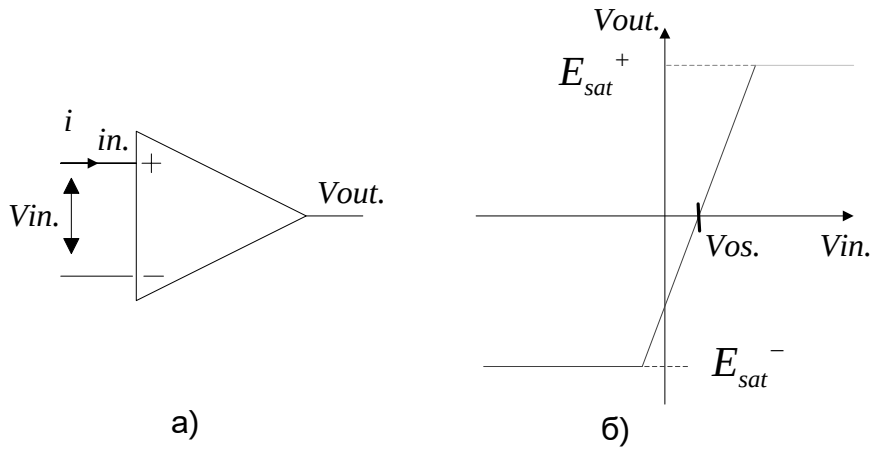


Рисунок 3.2 – Операційний підсилювач: графічне зображення (а) і передавальна характеристика

Оскільки реальний ОП містить компенсуючі і паразитні ємності, повна модель пристрою буде включати реактивні елементи. Однак, ми припустимо, що ОП поводиться як резистор в діапазоні частот, в якому працюватиме схема Чуа. Це завжди можна забезпечити відповідним масштабуванням часу, як це було показано раніше. Таким чином, ми нехтуємо усіма частотно-залежними ефектами в ОП і працюємо з ним як з чисто активним пристроєм [27].

Можна припустити також, що вихідний імпеданс ОП досить малий, так що ним можна знехтувати.

Таким чином, в наших цілях вихід ОП виглядає як ідеальне джерело напруги, а вхід - як розрив ланцюга. Тому ми можемо моделювати ОП як кероване напругою джерело напруги: $v_{in} = 0$; $v_{out} = f(v_{in})$, де $f(v)$ має вигляд, представлений на рисунку 3.3 б.

Перевагою даної кусково-лінійної моделі є те, що ми тепер можемо визначити поведінку ланцюга, утримуючої ОП та інші компоненти, аналізуючи кожну лінійну ділянку роботи (від'ємне насичення, лінійна область і позитивне насичення) окремо.

Як показано на рисунку 3.3, ОП моделюється як кероване напругою джерело напруги з трьохсегментною характеристикою перетворення напруги. У даній моделі враховується ненульовий постійний зсув v_{os}, кінцеве підсилення A в лінійній області і (можливо різні) рівні насичення $-E_{sat}^{-}$ і E_{sat}^{+}.

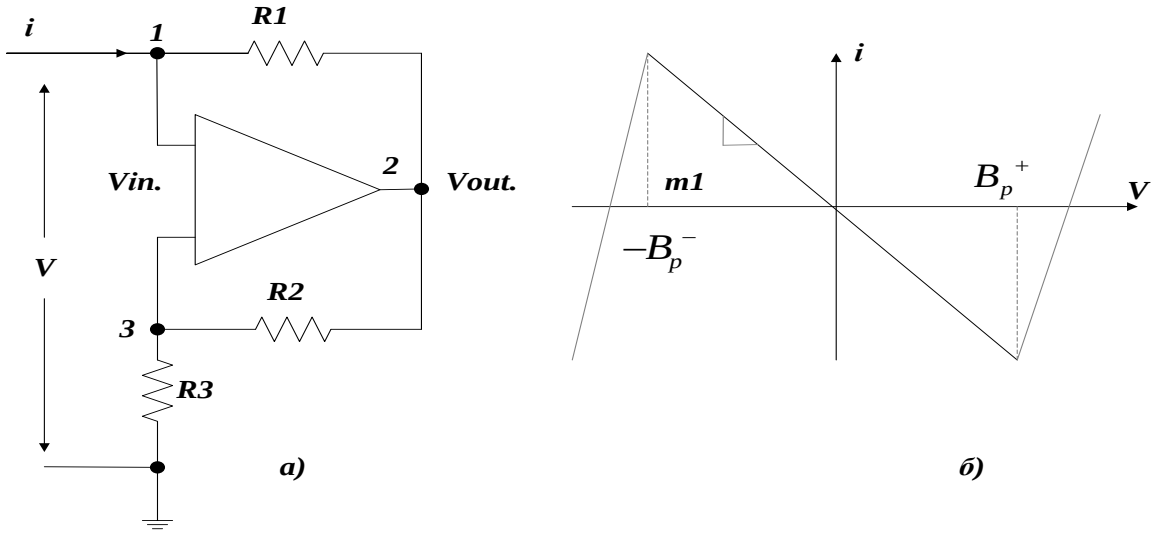


Рисунок 3.3 – Перетворюч від'ємного опору на основі операційного підсилювача: (а) принципова схема; (б) ВАХ перетворювача при умові,що характеристика ОП має вигляд, представлений на рисунку 3.2

Від’ємне насичення $\nu_{out} = -E_{sat}^{-}$ $\nu_{in} \le -\frac{E_{sat}^{-}}{A}$

Лінійна ділянка $\nu_{out} = A\nu_{in}$ $-\frac{E_{sat}^{-}}{A} \le \nu_{in} \le \frac{E_{sat}^{+}}{A}$

Додатнє насичення $\nu_{out} = E_{sat}^{+}$ $\nu_{in} \ge \frac{E_{sat}^{+}}{A}$

За законом Кірхгофа для струмів по неінвертуючому вході ОП (вузол 1) на рисунку 3.4 а запишем:

$$i = \frac{1}{R_1}(\nu - \nu_{out}) \tag{3.4}$$

Напруги в контурі 1-3-0-1 пов’язані співвідношенням:

$$\nu = \nu_{in} + \left[\frac{R_3}{R_2 + R_3}\right]\nu_{out} \tag{3.5}$$

Розглянемо окремо три лінійних ділянки характеристики перетворювача.

ОП при позитивному насиченні:

$$\nu_{out} = E_{sat}^{+}$$

Потім, підставляючи ν_{out} в 3.4, отримуємо:

$$i = \frac{1}{R_1}\nu - \frac{1}{R_1}E_{sat}^{+}$$

ОП знаходиться в позитивному насиченні при:

$$\nu_{in} \ge \frac{E_{sat}^{+}}{A}$$

Це співвідношення є умовою області позитивного насичення. Нам відомо, що $\nu = \frac{E_{sat}^{+}}{A} + \frac{R_3}{R_2 + R_3} E_{sat}^{+}$.

Тоді умови приймають вигляд:

$$\nu \geq \left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] E_{sat}^{+}$$

Це відповідає правому сегменту на ВАХ на рисунку 3 б. Точка зламу визначається як

$$B_p^{+} = \left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] E_{sat}^{+}$$

а нахил – як

$$m_0 = 1 / R_1$$

Для великих A,

$$B_p^{+} \approx \left[\frac{R_3}{R_2 + R_3} \right] E_{sat}^{+}$$

ОП в області негативного насичення. Підстановка $\nu_{out} = -E_{sat}^{-}$ замість $\nu_{out} = E_{sat}^{+}$ для наведеного вище аналізу дає крайній лівий сегмент ВАХ на рисунку 3.4б. $m_0 = 1 / R_1$, як і раніше, і умова від'ємного насичення має вигляд:

$$-B_p^{-} = \left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] E_{sat}^{-}$$

Це верхня межа області від'ємного насичення.

Лінійна область ОП. У лінійній області $\nu_{out} = A\nu_{in}$.

Підстановка v_{out} в 3.4 дає співвідношення

$$i = \frac{1}{R_1} v - \frac{1}{R_1} A v_{in} \tag{3.6}$$

Тепер із 3.5

$$v = v_{in} + \frac{R_3}{R_2 + R_3} v_{out} = v_{in} + \frac{R_3}{R_2 + R_3} A v_{out} = \left[\frac{R_2 + (1+A)R_3}{R_2 + R_3} \right] v_{in}$$

Виразив v_{in} через v, отримуємо:

$$v_{in} = \left[\frac{R_2 + R_3}{R_2 + (1+A)R_3} \right] v \tag{3.7}$$

Підстановка v_{in} в залежності від v в 3.6 дає:

$$i = \left[\frac{(1-A)R_2 + R_3}{R_1 \left[R_1 + (1+A)R_3 \right]} \right] v$$

Для великих A,

$$i \approx -\left[\frac{R_2}{R_1 R_3} \right] v$$

ОП працює в лінійній області, коли $-\frac{E_{sat}^{-}}{A} \le v_{in} \le \frac{E_{sat}^{+}}{A}$

Або, підставляючи вираз для v_{in} з 3.7:

$$-\frac{E_{sat}^{-}}{A} \le v_{in} = \left[\frac{R_2 + R_3}{R_2 + (1+A)R_3} \right] v \le \frac{E_{sat}^{+}}{A}$$

Звідси, ОП працює в лінійній області, коли:

$$-\left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] E_{sat}^{-} \le v \le \left[\frac{R_2 + (1+A)R_3}{A(R_2 + R_3)} \right] E_{sat}^{+}$$

Для великих A рівняння зводиться до вигляду:

$$-\left[\frac{R_3}{R_2+R_3}\right]E_{sat}^{-} \le v \le \left[\frac{R_3}{R_2+R_3}\right]E_{sat}^{+}$$

Розглянемо ще раз рисунок 3.4 б. Ми маємо:

$$m_1 = \left[\frac{(1-A)R_2+R_3}{R_1\left[R_2+(1+A)R_3\right]}\right]$$

При великих значеннях A, отримуємо:

$$m_1 \approx -\left[\frac{R_2}{R_1R_3}\right]$$

Вольт-амперна характеристика є кусково-лінійною і складається з трьох сегментів. Як і колись, ми припускаємо, що A велике. Тоді центральна частина має нахил $m_1 \approx -R_2/(R_1R_3)$,а зовнішні області (відповідні насиченню ОП – внаслідок пасивності в загальному) мають нахили $m_0 = 1/R_1$. Якщо $R_2 = R_1$, тоді $m_1 = 1/R_3$.

Надалі будемо припускаємо, що рівні насичення ОП рівні за величиною. Таким чином, $E_{sat}^{+} = E_{sat}$; $-E_{sat}^{-} = -E_{sat}$ у відповідності з припущенням, а точки зламу розташовані в $\pm(R_3/R_2+R_3))E_{sat}$.

Перетворювач від'ємного опору (ПВО) на ОП буде основним блоком діода Чуа. Для того, щоб отримати нелінійну характеристику, представлену на рисунку 3.5, необхідно з'єднати паралельно два таких перетворювачі від'ємного опору, як це показано на рисунку 3.4, (та наведено в додатку А рис.9).

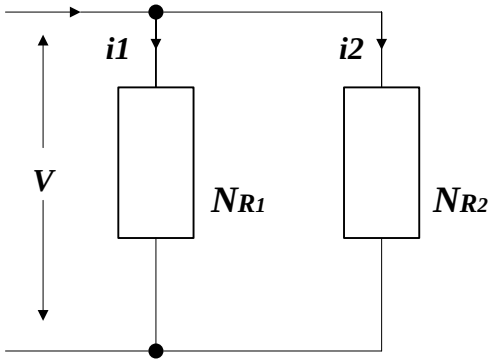


Рисунок 3.4 – Паралельне з’єднання двох кусково-лінійних резисторів

Нехай обидва управляються напругою. Струм i_1, що протікає через резистор N_{R_1}, коли до його виводів прикладено напругу v_1, визначається залежністю $i_1 = f_1(v_1)$.

Точно так же струм $i_2 = f_2(v_2)$ тече в N_{R_2}. Загальний струм задається функцією $i = g(v)$, де $g(v) = f_1(v) + f_2(v)$.

Таким чином, паралельне з’єднання двох (або більше) керованих напругою нелінійних резисторів також є кероване напругою нелінійних резисторів. Визначити форму $g(v)$ можна графічно складанням i_1 та i_2 для всіх v, як показано на рисунку 3.5.

Цей спосіб дозволяє сконструювати пятисегментний фізично реалізований кусково-лінійний резистор, необхідний для схеми Чуа, шляхом паралельного з’єднання двох перетворювачів негативного опору з ВАХ відповідної форми [28].

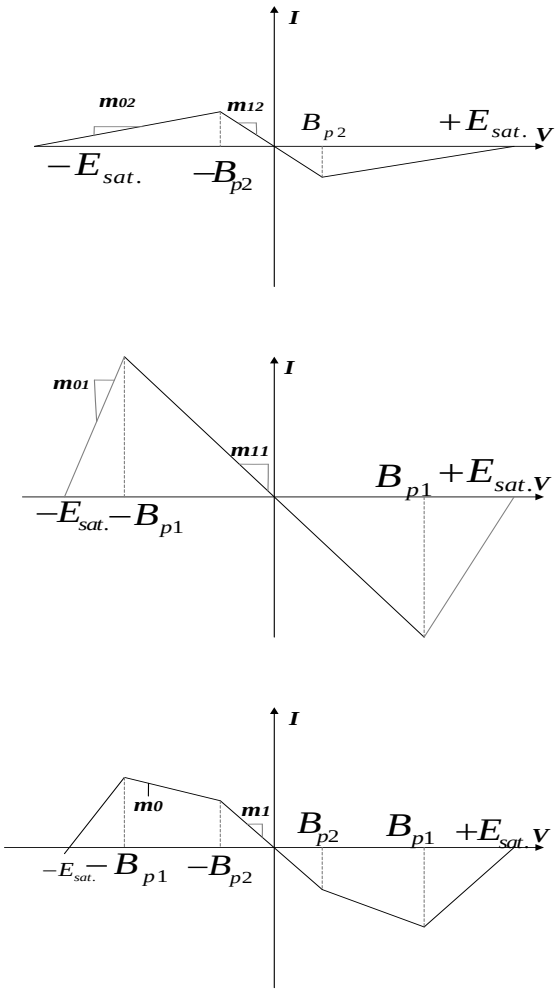


Рисунок 3.5 Графічне представлення двох вольт-амперних характеристик нелінійних резисторів

3.3 Реалізація схеми генератора Чуа на схемотехнічних аналогах приладів із від'ємним диференційним опором

На рисунку 3.6 (та наведена в додатку А рис.10) зображена реалізація ланцюга Чуа на ОП. Потрібна для діода Чуа ВАХ задається двома керованими напругою перетворювачами негативного опору, з'єднаними паралельно.

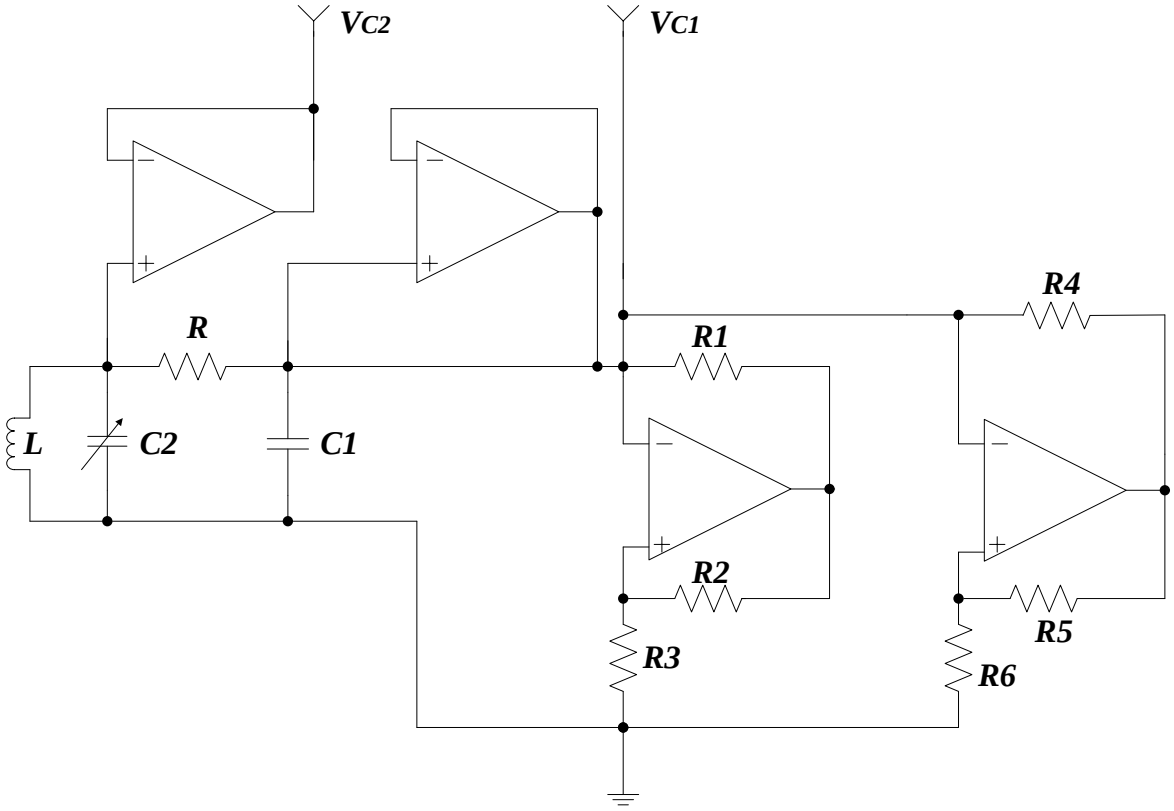


Рисунок 3.6 – Принципова схема системи Чуа. Додаткові ОП включені в схему для усунення впливу вимірювальних приладів на динаміку системи Чуа

Нелінійний резистор N_{R_1} має трьохсегментну кусково-лінійну характеристику з нахилами m_{0_1} і m_{1_1} і точками зламу $\pm B_{p_1}$ (як на рисунку 3.5б). Точно так же у N_{R_2} маються нахили m_{0_2} і m_{0_2},і точки зламу $\pm B_{p_2}$ (рисунок 3.5а). Складова п'ятисегментної характеристики має нахили m_{-1}, m_0 і m_1, і точки зламу $\pm B_{p_1}$ і $\pm B_{p_2}$ (як на рисунку 3.5 в).

На перетворювачі від'ємного опору на ОП ми побачили, що якщо $R_2 = R_1$ на рисунку 3.4 а, то будуть нахили R_1 і $-1/R_3$, з точками зламу $\pm(R_3/(R_2+R_3))E_{sat}$. Таким чином, при $R_2 = R_1$,

$$m_{0_1} = \frac{1}{R_1},\ m_{1_1} = -\frac{1}{R_3},\ \mathrm{B}_{p_1} = \frac{R_3}{R_2 + R_3} E_{sat}$$

Вважаючи, що $R_5 = R_4$, отримуємо наступне:

$$m_{0_2} = \frac{1}{R_4},\ m_{1_2} = -\frac{1}{R_6},\ \text{В}_{p_2} = \frac{R_6}{R_5 + R_6} E_{sat}$$

З графічного розгляду складової характеристик маємо:

$$m_{1_1} + m_{0_2} = m_0,$$
$$m_{1_1} + m_{1_2} = m_1.$$

За допомогою даних спостережень ми можемо вивести стратегію для визначення підходящих значень компонентів $R_1 - R_6$ з m_0, m_1 і B_{p_2}.

Вибір комплектуючих елементів.

E_{sat} визначається джерелом енергії і внутрішнім пристроєм ОП. Не обов'язково, щоб були відомі ці значення, але можна їх виміряти. Для діючої установки E_{sat} складає приблизно 14,2 В. Форма необхідної характеристики визначається значеннями B_{p_2}, m_0, m_1. Вибір величин B_{p_1} і m_{-1} до деякої міри довільний [29].

Виберемо R_1 досить великим, щоб він не навантажував сильно ОП (скажімо, 330 Ом). Розрахуємо $B_{p_1} = (1/(1-m_1 R_1))E_{sat}$. Якщо B_{p_1} недостатньо велике , щоб динаміка аттрактора залишалась в межах області негативного опору, потрібно зменшити R_1 і спробувати знову. Необхідно знайти довжину області негативного опору в залежності від величини R_1.

Будемо вважати, що $R_2 = R_1$. Знайдемо R_3:

$$R_3 = \frac{E_{sat}}{(B_{p_2} - E_{sat})m_0 - B_{p_2} m_1}$$

Розрахуємо R_4:

$$R_4 = \frac{E_{sat}}{B_{p_2}(m_0 - m_1)}$$

Будемо вважати, що $R_5 = R_6$. Знайдемо R_6:

$$R_6 = \frac{E_{sat}}{(E_{sat} - B_{p_2})(m_0 - m_1)}$$

Необхідна нелінійна характеристика визначається m_0 = -0,409 мСм, m_1 = -0,756 мСм і B_{p_2} =1,08 В.

3.4 Комп'ютерне моделювання схеми генератора Чуа в Micro-Cap

3.4.1 Часові діаграми сигналу на виході

Моделювання схеми проводилось, вважаючи, що вольт-амперні характеристики (ВАХ) для конденсаторів, резисторів та індуктивності є лінійними, а ВАХ нелінійного елемента є кусково-лінійною. Головним завданням при дослідженні є коректне моделювання нелінійного елемента. В нашому випадку нелінійність реалізована за допомогою нелінійного елемента (R_8), операційного підсилювача в сукупності з діодами [30].

Схема може демонструвати такі явища хаосу як біфуркації і хаотичний аттрактор. Для досягнення хаотичної поведінки між номіналами елементів потрібно дотримуватися певного співвідношення. Так, ємність конденсатора C_2 повинна бути приблизно в 10 разів більше ємностей C_1, співвідношення C_2 / C_1 називають α. Коефіцієнт β показує співвідношення між R, C_2 і L, а саме, $\beta = R \wedge 2 \cdot C_2 / L$ і повинен дорівнювати приблизно 15.

Тому для моделювання схеми генератора Чуа будемо використовувати компоненти з такими номіналами: C_1=470 нФ, C_2=47 нФ, L= 15 мГн, R_1= R_2=220 Ом, R_3= 2,2 кОм, R_4= R_5=22 кОм, R_6= R_7 =3,3 кОм, R_8=300 Ом, DA=TL082, VD_1=VD_2=1N914.

Результати комп'ютерного моделювання схеми генератора Чуа з використанням нелінійного елемента на операційному підсилювачі та діодах в програмному середовищі Micro-Cap.

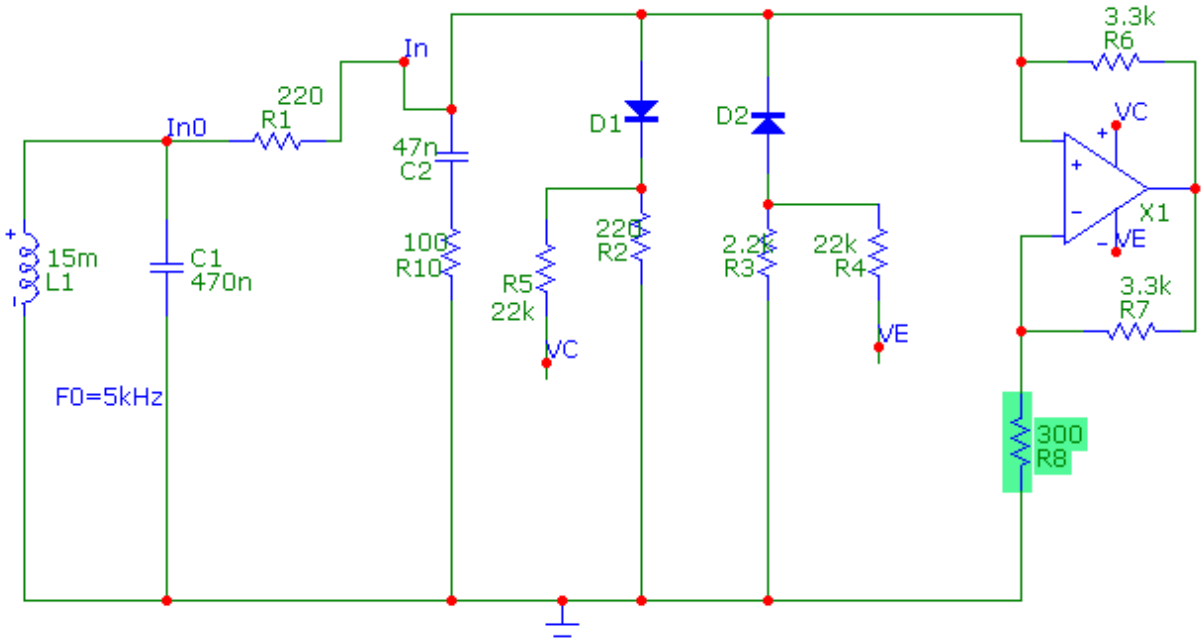


Рисунок 3.8 – Реалізація схеми генератора Чуа в програмному пакеті Micro-Cap

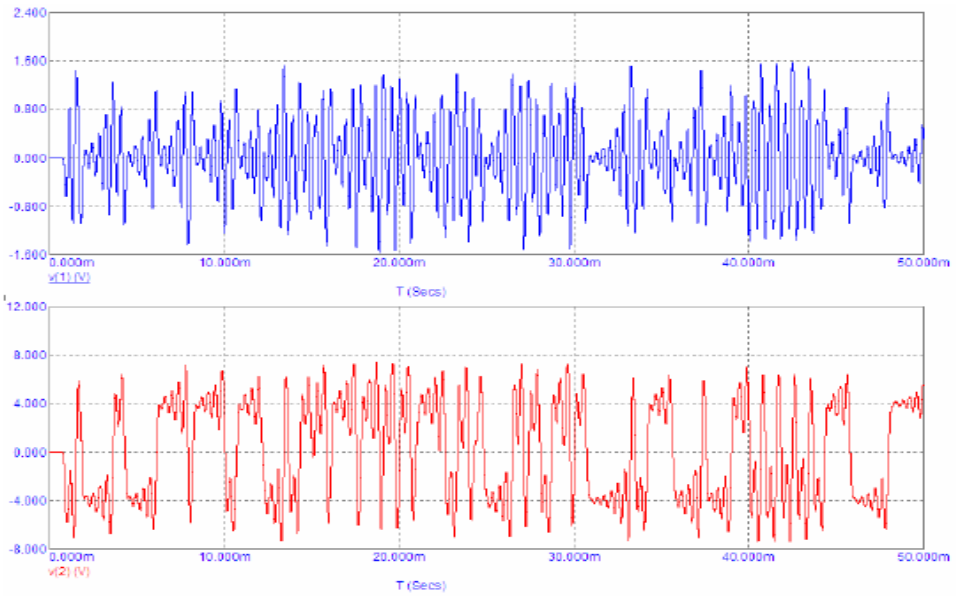


Рисунок 3.9 – Часова діаграма сигналу на виході генератора

Нелінійний опір реалізований на елементах U_1, U_2, D_1, D_2, R_1-R_6. Хоча ємність C_1 позитивна, завдяки впливу перерахованих вище елементів вона діє як від'ємна ємність.

3.4.2 Спектр сигналу на виході

Вихідні сигнали схеми генератора Чуа – це напруги на діодах Чуа D_1 та D_2. У передавачі напруга V_2 підсумовується з напругою V_1 синусоїдного джерела частотою 5 кГц, яка імітує інформаційне повідомлення. Номінали елементів схем Чуа в приймачі та передавачі збігаються. Сигнали будемо знімати з конденсаторів C_1 і C_2.

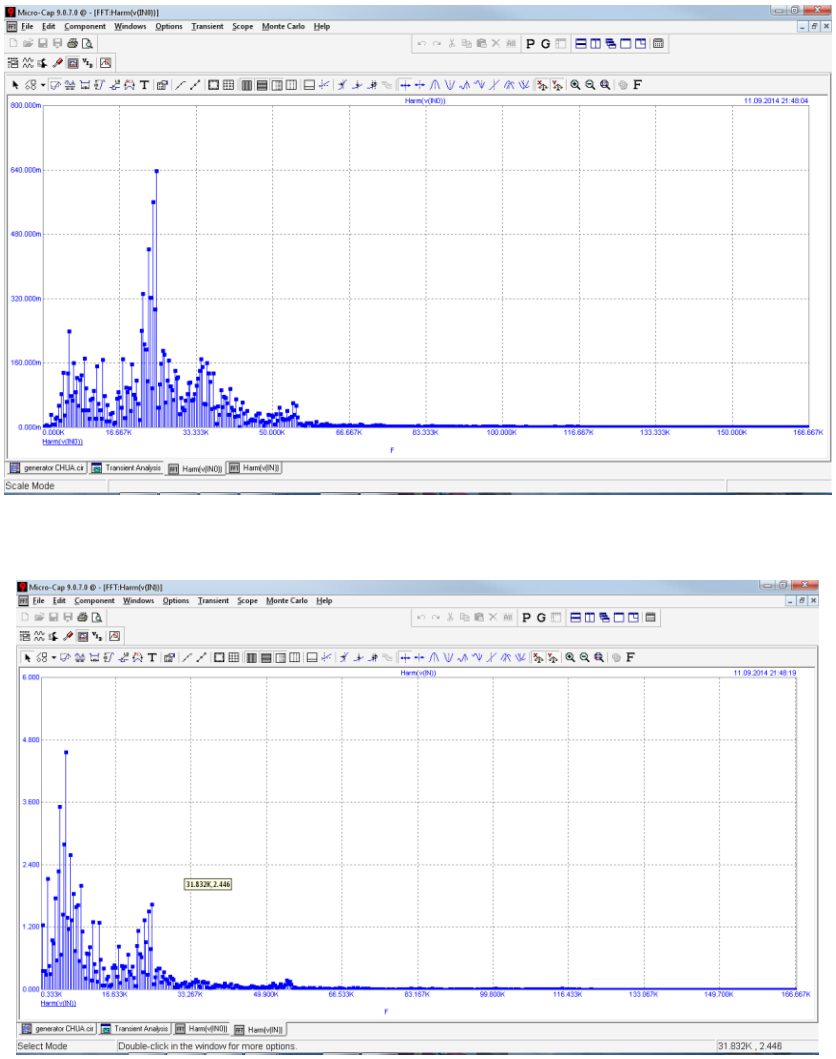


Рисунок 3.10 Спектральні характеристики генерованих схемою Чуа сигналів

Із спектральної характеристики сигналу бачимо, що в хаотичному режимі смуга генерації достатньо широка і має яскраво виражених піки.

Вихідні сигнали з часом відрізняються внаслідок накопичення похибок числового інтегрування. Це є проявом особливості дивного аттрактора. Тому для правильного відтворення інформаційного сигналу в приймачі необхідно час від часу вирівнювати значення змінних стану, тобто значення напруг на конденсаторах і струмів у індуктивностях.

3.4.3 Фазовий портрет досліджуваної схеми

Дослідимо поведінку ланцюга Чуа залежно від параметра R. Результати моделювання відображені на рис. 3.11(та наведено в додатку А рис.14), 3.12 (та наведено в додатку А рис.15).

Зменшуючи значення опору R_8 спостерігаємо, що точка перетворюється на орбіту. Подальше зменшення опору призводить до роздвоювання цієї орбіти, ми починаємо спостерігати біфуркації.Подвоєння періоду орбіти будуть відбуватися і далі із зменшенням опору, відстані між наступними роздвоєностями будуть постійно і планомірно зменшуватися.

Період, до якого вам вдасться спостерігати біфуркації залежить від чіткості сигналів.

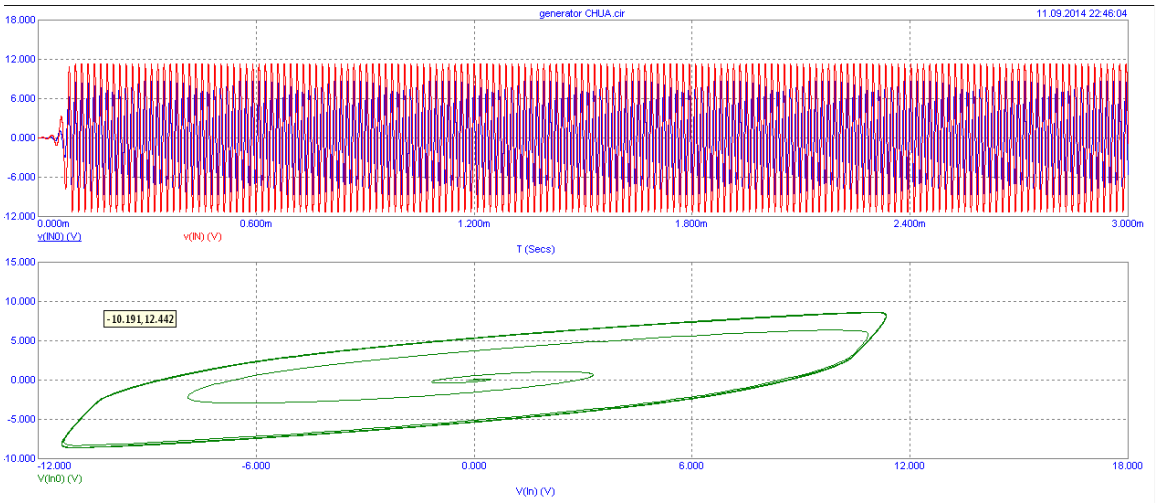


Рисунок 3.11 – Сигнал на виході генератора хаосу та його фазовий портрет

У якийсь момент стабільна орбіта поступається місце двопетлевому аттрактору, який знаменує настання хаосу. Цей аттрактор має три точки рівноваги: одну на початку координат, і дві в «дірках» петель (рисунок 3.12).

Типова траєкторія аттрактора починає обертання навколо однієї з «дірок», віддаляючись від точки рівноваги з кожним витком, потім траєкторія або повертається ближче в центру і знову видаляється, або направляється до іншої точки рівноваги, де процес повторюється. Кількість обертань в кожному випадку випадкове.

Спостерігається послідовність біфуркацій подвоєння періоду для аттрактора.

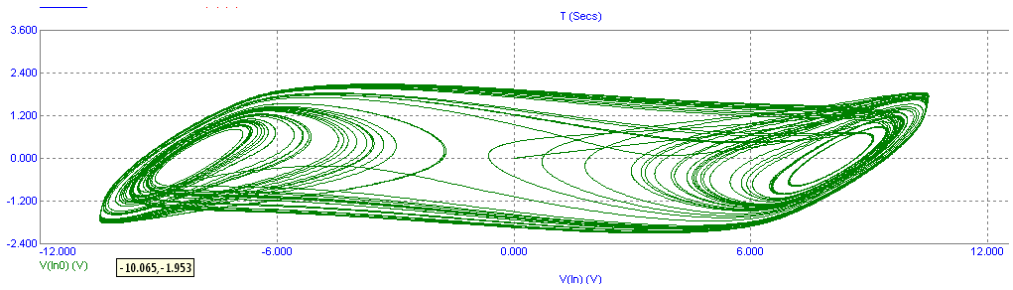


Рисунок 3.12 – Фазовий портрет аттрактора «подвійний виток»

3.5 Висновки до розділу

В ході виконання комп'ютерного моделювання було досліджено генератор хаотичних коливань та його властивості. Були отримані вихідні сигнали на виході генератора, спектр сигналу, а також фазові портрети аттрактора при різних значеннях опору. Досліджено, що зменшуючи значення опору R_8 призводить до того, що точка перетворюється на орбіту. Подальше зменшення опору призвело до роздвоювання цієї орбіти, спостерігалися біфуркації типу «подвійний виток».

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ПРИСТРОЮ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ХАОСУ

В даному розділі проводемо комп'ютерне моделювання схеми генератора Чуа, експериментально дослідимо хаотичну поведінку ланцюга Чуа, на основі побудованої структурної схеми експериментально дослідимо генератор хаосу, що реалізований на операційних підсилювачах і аналогових помножувачах сигналів за допомогою програмного пакету Micro-Cap.

4.1 Аналіз електричної принципової схеми

Розглянемо два ідентичні генератори хаосу, які зв'язані резистивним зв'язком [31]. Схема складається з 4-х конденсаторів, 2-х котушок індуктивностей, 18-ти резисторів, 3-ох операційних підсилювачів (ОП). Діод Чуа в для даній схемі, реалізований за допомогою 3-х операційних підсилювачів.

Схема для моделювання генератора Чуа з резистивним зв'язком в програмі Micro-Cap, приведена на рисунку 4.1.

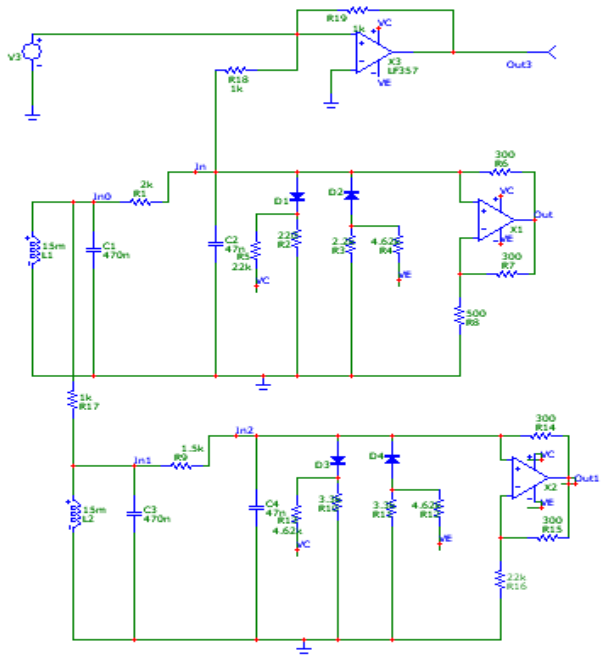


Рисунок 4.1 - Схема для моделювання процесів в системі двох ідентичних генераторів Чуа з резистивним зв'язком

За допомогою програми Micro-Cap було проведено дослідження даної схеми.

В ході моделювання були отримані осцилограми напруг і струмів на елементах системи.

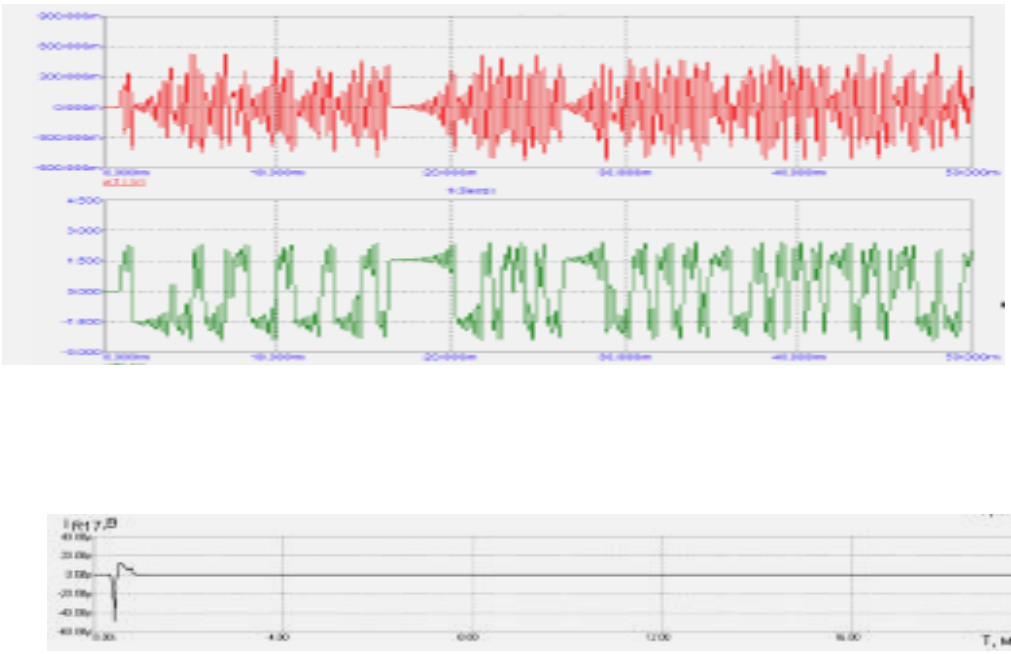


Рисунок 4.2 - Графіки напруг і струмів на елементах системи при резистивному зв’язку

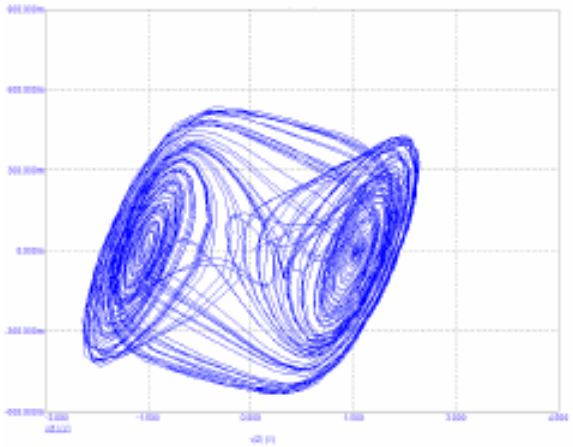


Рисунок 4.3 Дивний аттрактор типу «подвійний виток » в системі резистивно- пов’язаних генераторів Чуа

З рисунка 4.3 видно, що в разі резистивного зв'язку між генераторами виникають хаотичні коливання напруг і струмів. Крім того, хаотичні коливання на однойменних елементах генераторів Чуа є синхронними.

Ця обставина підтверджується тим, що струм з'єднує через генератори Чуа резистор в сталому режимі і буде дорівнювати нулю, отже, фазовий зсув між коливаннями на однойменних елементах відсутній. Фазовий портрет коливань на елементах є дивним аттрактором типу «подвійна спіраль».

4.2 Комп'ютерне моделювання та фазові портрети

4.2.1 Часові діаграми сигналів з генераторів хаосу в режимах відсутності та наявності синхронізації

Розглянемо процес синхронізації сигналів $y_1(t)$ і $y_2(t)$ ведучої і веденої систем. Ведуча і ведена системи формують хаотичні сигнали $x_1(t), y_1(t)$ та $x_2(t), y_2(t)$ [32].

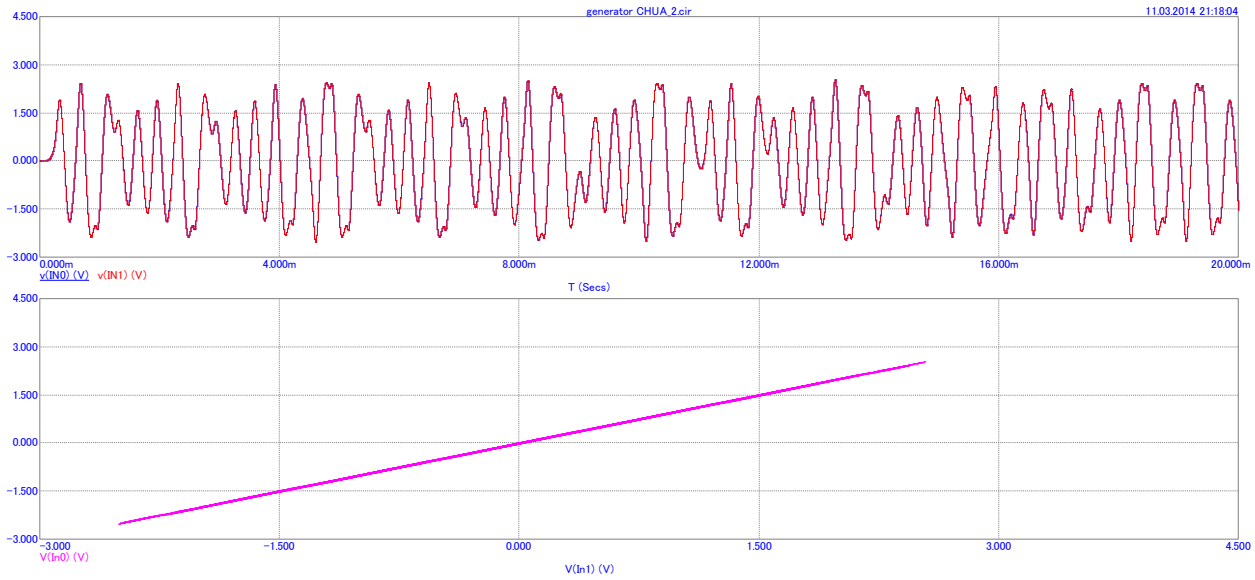
Для моделювання процесу синхронізації ведучої і веденої систем використовувалося програмне середовище Micro-Cap.

Глибина зв'язку між системами регулюється зміною величини опору R_x.

Наявність синхронізації досліджуваних систем підтверджується залежностями амплітуди сигналу веденої системи $y_2(t)$ від амплітуди сигналу ведучої $y_1(t)$, які наведені на рисунку 4.4, а: при $R_x = 100$ Ом залежність $y_2 = f(y_1)$ лінійна з кутом нахилу $\varphi = \pi/4$, що вказує на ідентичність сигналів.

Збільшення опору R_x до 3 кОм призводить до десинхронізації систем (рисунок 4,4, б).

а) синхронізація



а) десинхронізація

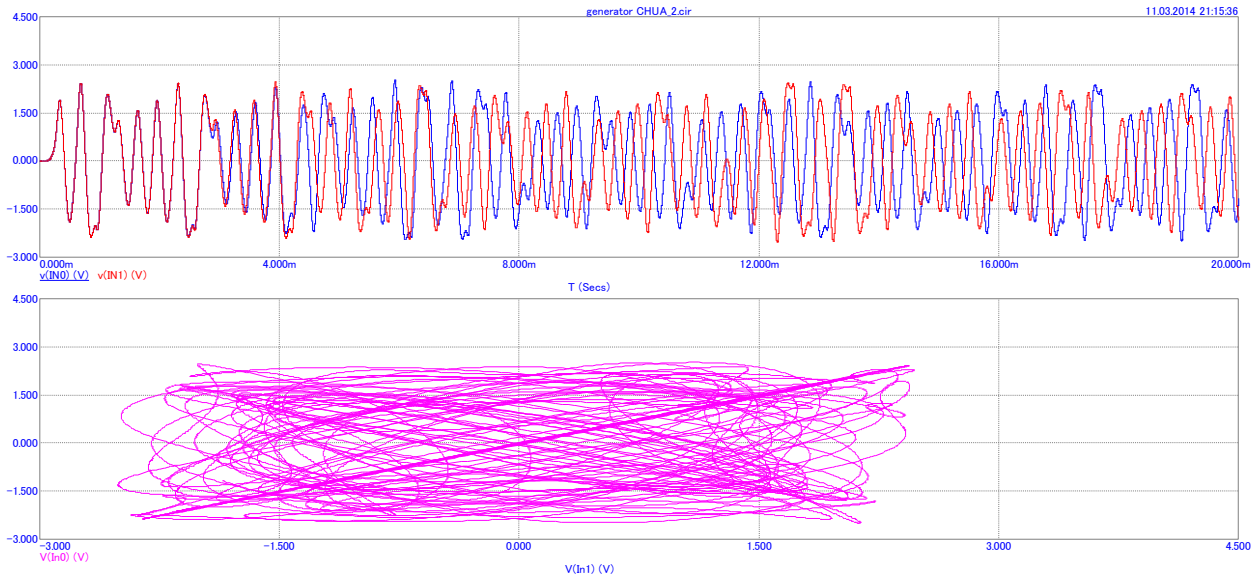
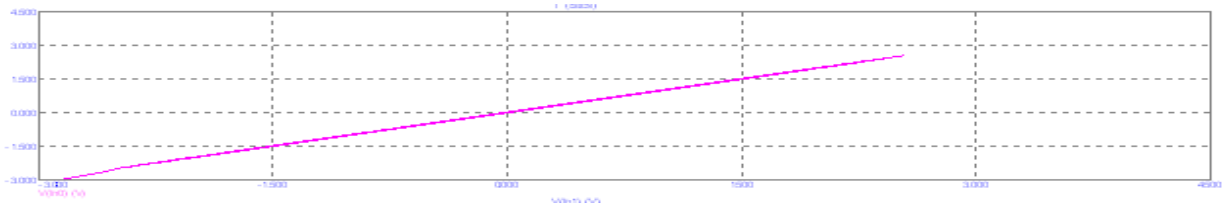


Рисунок 4.4 - Залежність амплітуди сигналу y_2 від амплітуди сигналу y_1 для досліджуваної системи при $R_x = 100$ Ом (а) і $R_x = 3$ кОм (б)

З результатів експериментальних досліджень режиму синхронізації ведучої та веденої систем, наведених на рисунок 4.4, випливає, що синхронізація сигналів $x_1(t)$ і $x_2(t)$ (рисунок 4.5,а) забезпечується встановленням синхронізації сигналів $y_1(t)$ і $y_2(t)$ (рисунок 4.5, б).

а)



б)

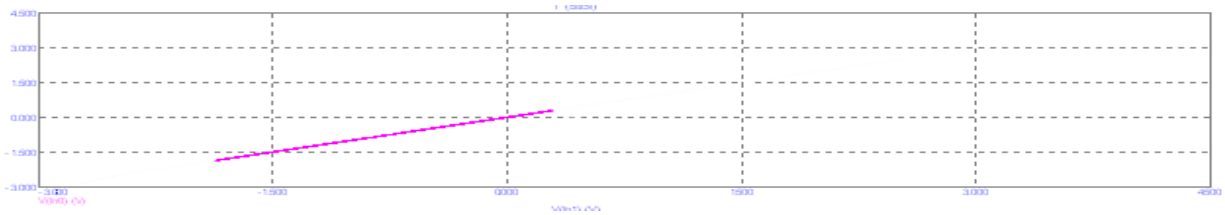


Рисунок 4.5 – Експериментальні залежності $x_2 = f(x_1)$ (а) і $y_2 = f(y_1)$ (б)

4.2.2 Аналіз структурної схеми СЗІ з використанням генератора хаосу

В основу схеми поставлена задача створити спосіб закритої передачі інформації в системі радіозв'язку шляхом застосування перемноження та інтегрування хаотичного сигналу, який забезпечить підвищення скритності та перешкодостійкості системи радіозв'язку.

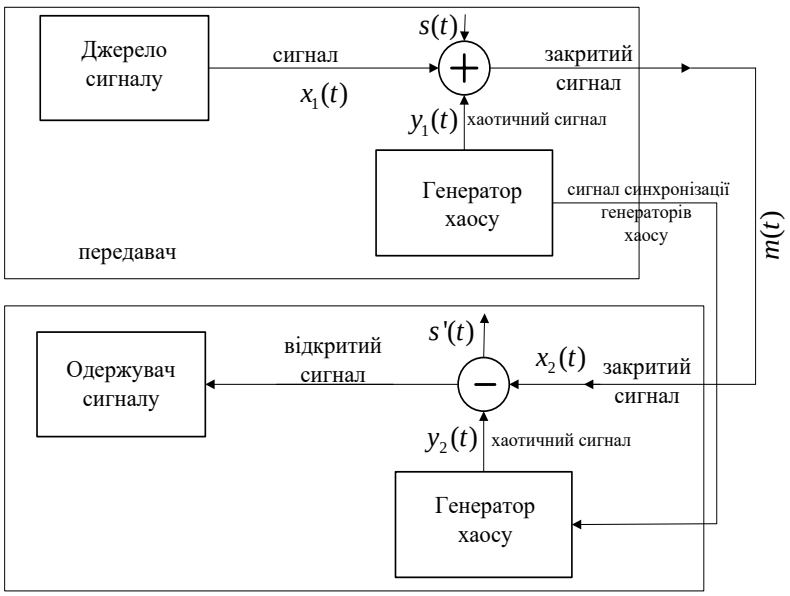


Рисунок 4.6 – Структурна схема генератора хаосу

На передавальній стороні формується синусоїдальний інформаційний сигнал сигнал, який адитивно підмішується до хаотичного сигналу в суматорі на виході передавальної системи, після чого результуючий сигнал передається по каналу зв'язку. Синхронізація системи зв'язку здійснюється встановленням однакових динамічних режимів роботи приймальної і передавальної частин системи зв'язку за допомогою переданого і ідентичного йому сигналу, згенерованого приймальною стороною. На приймальній стороні відбувається детектування інформаційного сигналу шляхом вирахування від прийнятого сигналу синхровідгуку. На рисунку 4.6 наведено структурну схему передачі інформації з використанням генератора хаосу, (та наведена в додатку А рис.16).

Нелінійний передавач системи складається із генератора хаотичних коливань і блоку підсумовування сигналів, а приймач - з ідентичного генератора і блоку віднімання.

Генератори хаотичних коливань ведучої і веденої систем формують сигнали $x_1(t), y_1(t)$ і $x_2(t), y_2(t)$, що мають властивості хаотичної динаміки. Синхронізація сигналів $x_1(t)$ і $x_2(t)$ системи забезпечується шляхом встановлення синхронізації сигналів $y_1(t)$ і $y_2(t)$ за допомогою схеми лінійного зворотного зв'язку. Інформаційний сигнал $s(t)$ підсумовується з несучим хаотичним сигналом $y_1(t)$ і передається по лінії зв'язку (закритий сигнал). В якості інформаційного сигналу подається синусоїда з амплітудою
3В і частотою 600 Гц. На приймальній частині системи відбувається віднімання від модульованого сигналу $m(t)$ синхронізованого хаотичного сигналу $x_2(t)$, в результаті чого отримуємо вихідний інформаційний сигнал. Відтворені вихідні дані надходять до отримувача інформації (відкритий сигнал).

4.2.3 Часові діаграми сигналів системи захисту інформації

Принципова схема СЗІ з використання генераторів хаосу з резистивним зв’язком представлена на рисунку 4.7.

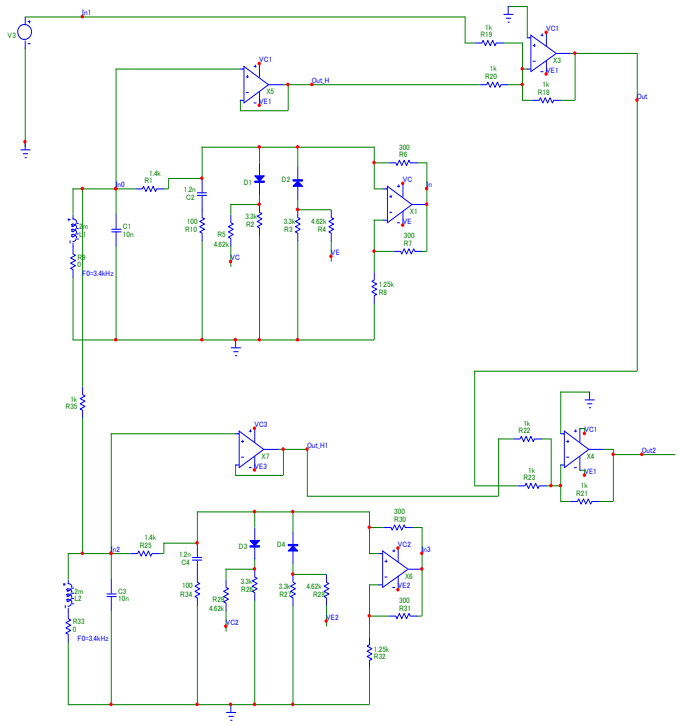


Рисунок 4.7 – Принципова схема СЗІ з використанням генераторів хаосу

Експериментально система передачі інформації була реалізована на операційних підсилювачах. В блоках сумування і віднімання сигналів перший операційний підсилювач виконує функцію буфера.

В якості інформаційного сигналу подали синусоїду з амплітудою 1 В і частотою 3,4 кГц. При моделюванні припускалось, що канал зв’язку є ідеальним. Отримали в результаті моделювання часові діаграми амплітуд сигналів (в вольтах) та їх спектри:

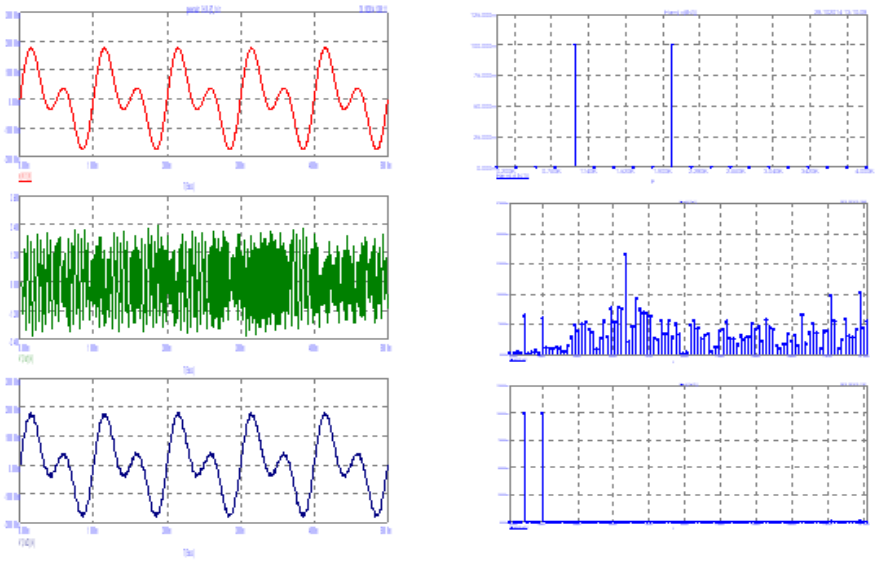


Рисунок 4.9 – Часові діаграми та спектри сигналів: а) вхідного інформаційного сигналу; б) закритого сигналу; в) розшифрованого сигналу (правильно)

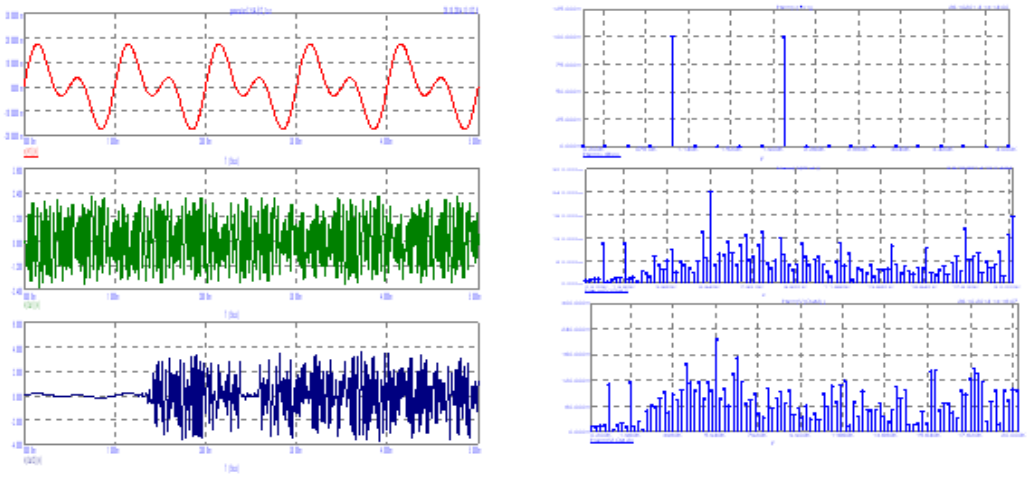


Рисунок 4.10 – Часові діаграми та спектри сигналів: а) вхідного інформаційного сигналу; б) закритого сигналу; в) розшифрованого сигналу (неправильно)

Ключем до розшифрування інформаційного сигналу є параметри схеми та сигнал синхронізації.

Відомо що, в звичайних системах зв’язку шум погіршує якість прийому, а при підсумовуванні хаотичного сигналу з інформаційним обставина зворотня: чим більше хаосу, тим краща якість хаотичної синхронізації і краща якість прийнятого сигналу.

З отриманих в результаті моделювання часових діаграм та спектрів сигналу, наведених на рисунку 4.9 (та наведено в додатку А рис.17), на рис. 4.10 (та наведено в додатку А рис.18) випливає, що вихідний сигнал на приймальній стороні збігається з вхідним інформаційним сигналом.

4.3 Висновки до розділу

В даному розділі було проведено комп’ютерне моделювання схеми генератора Чуа з резистивним зв’язком. Були отримані хаотичні коливання на однойменних елементах генераторів Чуа, які є синхронними, а також фазовий портрет типу «подвійний виток». Отримали часові діаграми сигналів з генераторів хаосу в режимах відсутності та наявності синхронізації. Було виявлено, що збільшення опору R_x призводить до десинхронізації систем.

Досліджено систему захисту інформації, що експериментально реалізована на операційних підсилювачах і помножувачах сигналів.Отримані часові діаграми та спектри сигналу показали, що вихідний сигнал на приймальній стороні збігається з вхідним інформаційним сигналом, що свідчить про захисні властивості даної системи.

Таким чином, це свідчить про те що, що генератори хаосу, побудовані на вирішенні рівнянь динамічних систем, успішно можуть використовуватися для захисту інформації.

5 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота на тему «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

5.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Початок XXI століття називають епохою становлення інформаційного або постіндустріального суспільства. У цій фазі розвитку цивілізації головними продуктами виробництва стають не речі й енергія, а інформація і знання. Одними із основних рис такого суспільства є: 1) збільшення питомої ваги інформаційно-комунікативних технологій, продуктів і послуг у валовому внутрішньому продукті країни; 2) поява якісно нових комунікацій та ефективної інформаційної взаємодії людей на засадах зростаючого доступу до національних і світових інформаційних ресурсів.

Тому вимоги до технологій і засобів зв’язку в сучасних умовах надзвичайно високі. Однією з основних проблем є забезпечення високої надійності (вірності) передачі даних при якомога більш високій швидкості. Якщо до того ж врахувати необхідність транспортування інформації в глобальних масштабах та проблеми взаємодії на цьому шляху різноманітних систем і мереж, то стає зрозумілим, що єдино можливим напрямком розвитку телекомунікацій є розробка високоефективних новітніх методів і засобів цифрового зв’язку.

Застосування сигналів складної форми дозволило підійти до вирішення важливої проблеми сучасних телекомунікаційних систем – захисту переданої інформації на фізичному рівні. Найбільш перспективними (з точки зору структурної скритності та захищеності інформації) типами систем є системи з хаотичним носієм.

Метою проведення комерційного і технологічного аудиту дослідження за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 5.1 [29].

Таблиця 5.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї

9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовують ся у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуютьс я у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці 5.2.

Таблиця 5.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	5	4	5
2. Ринкові переваги (наявність аналогів)	3	3	3
3. Ринкові переваги (ціна продукту)	4	4	4
4. Ринкові переваги (технічні властивості)	3	3	3
5. Ринкові переваги (експлуатаційні витрати)	3	3	3
6. Ринкові перспективи (розмір ринку)	4	3	3
7. Ринкові перспективи (конкуренція)	4	4	4
8. Практична здійсненність (наявність фахівців)	5	5	5

9. Практична здійсненність (наявність фінансів)	2	3	2
10. Практична здійсненність (необхідність нових матеріалів)	4	5	5
11. Практична здійсненність (термін реалізації)	5	4	5
12. Практична здійсненність (розробка документів)	5	5	4
Сума балів	47	46	46
Середньоарифметична сума балів $СБ_c$	46,3		

За результатами розрахунків, наведених в таблиці 5.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 5.3 [29].

Таблиця 5.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ ,розрахована на основі висновків	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» становить 46,3 бала, що, відповідно до таблиці 5.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

5.2 Оцінювання рівня новизни розробки

Виводячи на ринок новинку виробник вважає, що тієї новизни, якою наділена нова розробка є достатньо для того, щоб вона була сприйнята споживачем як нова. Але це не завжди так, в силу того, що споживач і виробник неоднозначно визначать її рівень новизни. Тому доцільним є визначення рівня новизни розробки отриманої в результаті досліджень за

темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань».

Саме визначення рівня і ступеня інтегральної новизни є найбільш актуальним, оскільки її рівень визначає ступінь однакового позитивного сприйняття новизни розробки як виробником, так і споживачем, а отже і ринком в цілому, а це, у свою чергу, є гарантією того, що новинка знайде своє місце на ринку, користуватиметься попитом у споживачів і забезпечить відшкодування витрат, зазнаних товаровиробником під час розроблення та виробництва технічної розробки [30].

Рівень новизни нової продукції розраховуємо експертним методом шляхом протиставлення нової продукції та її аналогів, що існують в даний час на ринку, за чинниками що визначають її значення, в системі «краще-гірше». Рівень новизни встановлюємо відносно рівня аналога (або продукту, що досить близький до аналога).

Для визначення *і*-го виду новизни, застосуємо чинники, які впливають на її рівень. Кожен чинник *і*-го виду новизни розраховуємо в балах. Більша кількість набраних балів свідчить про більший рівень новизни. Для оцінювання рівня новизни використаємо думки експертів, які встановлюють визначені бали відповідним чинникам. Бал відповідності проставляється в діапазоні від (-5 – значно гірше аналога до +5 – значно краще аналога). Результати попереднього оцінювання зведемо до відповідного листа оцінювання (таблиця 5.4).

Таблиця 5.4 – Лист оцінювання рівня новизни експертами

Види та чинники		Бали та експерти		
		Експерт 1	Експерт 2	Експерт 3
1		*2*	*3*	*4*
Споживча новизна	Питома вага 0,26	Максимальний бал $Б_{i\ MAX}$		25
1. Зміна поведінкових звичок споживача		2	2	2
2. Ступінь задоволення потреб і запитів		4	4	4
3. Спосіб задоволення потреби		2	2	2

Продовження таблицы 5.4 – Лист оцінювання рівня новизни експертами

4. Формування нової потреби		4	3	3
5. Формування нового споживача		0	0	0
Середній бал експертів $Б_{i\ отр}$		11		
Товарна новизна	Питома вага 0,21	Максимальний бал $Б_{i\ MAX}$		30
1. Параметричні зміни показників продукції				
1.1. Якісні		3	3	4
1.2. Технічні		3	4	3
1.3. Економічні		3	3	3
1.4. Сервісні		4	4	4
2. Якість продукції по відношенню до конкурентів		3	3	3
3. Функціональні зміни		4	4	4
Середній бал експертів $Б_{i\ отр}$		21		
Виробнича новизна	Питома вага 0,014	Максимальний бал $Б_{i\ MAX}$		25
1. Рівень унікальності товару для підприємства		5	5	5
2. Рівень унікальності для галузі		3	3	3
3. Рівень унікальності товару для країни		1	1	1
4. Зміна виробничої системи		4	4	4
5. Відносно існуючого асортименту		3	2	3
Середній бал експертів $Б_{i\ отр}$		16		
Прогресивна новизна	Питома вага 0,2	Максимальний бал $Б_{i\ MAX}$		25
1. Зміна технології виготовлення		4	4	4
2. Рівень застосування нових компонентів і матеріалів		0	0	0
3. Зміна технологічного принципу дії виробу		1	2	1
4. Зміна конструктивного виконання		3	3	3
5. Рівень застосування інновацій		2	2	2
Середній бал експертів $Б_{i\ отр}$		10		
Ринкова новизна	Питома вага 0,1	Максимальний бал $Б_{i\ MAX}$		20
1. Новий виріб на новому ринку		0	0	0
2. Новий виріб на відомому ринку		4	4	4
3. Модернізований виріб		3	3	3
4. Нова модель		1	1	1
Середній бал експертів $Б_{i\ отр}$		8		

Продовження таблиці 5.4 – Лист оцінювання рівня новизни експертами

Екологічна новизна	Питома вага 0,035	Максимальний бал $Б_i$ $_{MAX}$		20
1. Рівень екологічної чистоти технології виробництва		5	5	5
2. Рівень впровадження мало- та безвідходних технологій		5	5	5
3. Рівень екологічно небезпечних режимів експлуатації продукції		5	5	5
4. Рівень забруднення навколишнього середовища		5	5	5
Середній бал експертів $Б_{i\ отр}$		20		
Соціальна новизна	Питома вага 0,036	Максимальний бал $Б_i$ $_{MAX}$		20
1. Використання нового товару приводить до покращення стану здоров'я нації		0	0	0
2. Використання нового товару приводить до зростання доходів населення		0	0	0
3. Виробництво нового товару приводить до збільшення (зменшення) кількості робочих місць на підприємстві		4	5	4
4. Виробництво нового товару приводить до підвищення кваліфікації персоналу		3	4	3
Середній бал експертів $Б_{i\ отр}$		8		
Маркетингова новизна	Питома вага 0,145	Максимальний бал $Б_i$ $_{MAX}$		20
1. Нові методи маркетингових досліджень		0	0	0
2. Вживання нових стратегій сегментації ринку		3	3	3
3. Вибір нової маркетингової стратегії обхвату і розвитку цільового сегмента		1	1	1
4. Побудова нових каналів збуту		2	1	1
Середній бал експертів $Б_{i\ отр}$		5		

Значення *i*-го виду новизни розрахуємо за формулою [30]

$$I_i = \frac{Б_{i\,отр}}{Б_{i\,MAX}}, \tag{5.1}$$

де $Б_{i\ отр}$ – отримана кількість балів за шкалою оцінок чинників, що визначають *i*-й вид новизни;

$Б_{i\ max}$ – максимальна кількість балів, що може бути отримана за *i*-м видом новизни.

Загальний рівень інтегральної новизни розраховуємо шляхом перемноження отриманого значення *i*-го виду новизни на її вагомість, причому вагомість *i*-го виду новизни визначаємо експертним методом, за формулою [30]

$$N_{інт} = \sum_{i}^{n} W_i \cdot I_i \ , \tag{5.2}$$

де $N_{інт}$ – рівень інтегральної (сукупної) новизни;

W_i – вагомість (питома вага) *i*-го виду новизни;

n – загальна кількість видів новизни.

$$N_{інт} = (0{,}26 \cdot 11/25)+(0{,}21 \cdot 21/30)+(0{,}014 \cdot 16/25)+(0{,}2 \cdot 10/25)+(0{,}1 \cdot 8/20)+$$
$$(0{,}035 \cdot 20/20)+(0{,}036 \cdot 8/20)+(0{,}145 \cdot 5/20) = 0{,}481.$$

Отримане значення інтегрального рівня новизни зіставляємо зі шкалою, що наведена в табл. 5.5 [29].

Таблиця 5.5 – Рівні новизни нового товару та їхня характеристика

Рівні новизни товару	Значення інтегральної новизни	Характеристика товару	Вид нового товару
Найвища	1,00	Абсолютно новий товар	Новий товар, що наділений ознаками інноваційності (інноваційний товар)
Висока	0,8…0,99	Товар, який не має аналогів	
Значуща	0,6…0,79	Принципова зміна споживчих властивостей товару	
Достатня	0,4…0,59	Принципова технологічна модифікація товару	
Незначна	0,2…0,39	Кардинальна зміна параметрів	Новий товар
Помилкова	0,00…0,19	Малоістотна модифікація	

Згідно таблиці 6.5 розробка відповідає рівню при значенні інтегральної новизни 0,481 - достатня новизна; за характеристикою: принципова технологічна модифікація товару; вид розробки - новий товар, що наділений ознаками інноваційності (інноваційний товар).

5.3 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою [30]

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i , \tag{5.3}$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховуємо за такими формулами:

- для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки

$$\beta_i = \frac{I_{нi}}{I_{ai}} , \tag{5.4}$$

де $I_{ні}$ та $I_{на}$ – чисельні значення конкретного *i*-го технічного показника якості відповідно для нової розробки та аналога;

- для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки

$$\beta_i = \frac{I_{ai}}{I_{ні}}; \qquad (5.5)$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до табл. 5.6.

Таблиця 5.6 – Порівняння основних параметрів розробки та аналога

Показники (параметри)	Одиниця вимірювання	Аналог	Проектований пристрій	Відношення параметрів нової розробки до аналога	Питома вага показника
Кількість захищених телефонних ліній	Шт	4	8	2	0,4
Смуга пропускання каналів зв'язку	кГц	1,5	3	2	0,25
Відношення напруги спец. сигналу, що генерується приладом по лінії, до напруги спец. телефонного сигналу	дБ	50	60	1,2	0,1
Перехідне загасання між каналами приладу в робочому діапазоні частот, не менше	дБ	100	100	1	0,1
Час напрацювання на відмову,	год.	8000	10000	1,25	0,15

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 2 \cdot 0{,}4 + 2 \cdot 0{,}25 + 1{,}2 \cdot 0{,}1 + 1 \cdot 0{,}1 + 1{,}25 \cdot 0{,}15 = 1{,}71.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,71 рази.

5.4 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов'язані з проведенням науково-дослідної роботи на тему «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

5.4.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [29]

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (5.6)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, (грн.);

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=22 дні.

$$З_о = 14150{,}00 \cdot 22 / 22 = 14150{,}00 \ (грн.).$$

Проведені розрахунки зведемо до таблиці 5.7.

Таблиця 5.7 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	14150,00	643,18	22	14150,00
Старший науковий співробітник	13500,00	613,64	22	13500,00
Консультант (інженер систем технічного захисту інформації)	12650,00	575,00	6	3450,00
Інженер-дослідник (розробник мікроелектронної апаратури)	12000,00	545,45	22	12000,00
Технік І-ї категорії	7120,00	323,64	18	5825,45
Лаборант	6800,00	309,09	10	3090,91
Всього				52016,36

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» розраховуємо за формулою

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \qquad (5.7)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, (грн/год.);

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (5.8)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=6700,00 (грн.);

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) **[**29];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 22 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}35 / (22 \cdot 8) = 56{,}53 \ (грн.).$$

$$З_{р1} = 56{,}53 \cdot 7{,}20 = 407{,}03 \ (грн.).$$

Таблиця 5.8 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Установка обладнання	7,20	2	1,10	56,53	407,03
Підготовка робочого місця розробника мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань	5,30	3	1,35	69,38	367,71

Продовження таблиці 5.8 – Величина витрат на основну заробітну плату робітників

Встановлення програмного забезпечення розробки електронних схем	6,40	5	1,70	87,37	559,15
Підготовка бази даних	12,30	4	1,50	77,09	948,18
Монтаж компонентів мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань	4,60	5	1,70	87,37	401,89
Випробування дослідних блоків	2,50	5	1,70	87,37	218,42
Налагодження системи	1,30	3	1,35	69,38	90,19
Технічна підтримка експериментів	5,52	4	1,50	77,09	425,53
Всього					3418,08

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (5.9)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$$З_{дод} = (52016,36 + 3418,08) \cdot 11 / 100\% = 6097,79 \text{ (грн.)}.$$

5.4.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (5.10)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (52016,36 + 3418,08 + 6097,79) · 22 / 100% = 13537,09 (грн.).

5.4.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj}\,, \qquad (5.11)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, (грн/кг.);

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, (грн/кг.).

$М_1$ = 2,0 · 220,00 · 1,1 - 0 · 0 = 484,00 (грн.).

Проведені розрахунки зведемо до таблиці 5.9.

Таблиця 5.9 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний А4, Pro80, клас С, 500 л, UPM	220,00	2,0	-	-	484,00
Папір офісний А3, Maestro клас В, 80 г/м2, 500 л, Mondi	456,00	1,0	-	-	501,60
Папір офісний Офіс А5 80г/м2 500 аркушів клас С	125,00	3,0	-	-	412,50
Органайзер для канцелярського начиння	209,00	2,0	-	-	459,80
ДИСК CD-R VERBATIM 700MB 80MIN 52X BULK 50	15,20	4,0	-	-	66,88
USB флеш накопичувач 32 ГБ	172,00	1,0	-	-	189,20
Склотекстоліт СТФ 2–1.5	126,00	0,1	-	-	13,86
Хлорне залізо	190,00	0,100	-	-	20,90
Дріт монтажний	90,00	0,100	-	-	9,90
Лак УР-231	345,00	0,050	-	-	18,98
Спирт етиловий	170,00	0,250	-	-	46,75
Припій ПОС-61	528,00	0,03	-	-	17,42
Флюс БС-2	165,00	0,01	-	-	1,82
Всього					2263,24

5.4.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Мікроелектронний пристрій для технічного захисту інформації з

використанням генератора хаотичних коливань», розраховуємо, згідно з їхньою номенклатурою, за формулою

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (5.12)$$

де $Н_j$ – кількість комплектуючих j-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих j-го виду, (грн.);

$К_j$ – коефіцієнт транспортних витрат, ($К_j = 1,1 \ldots 1,15$).

$$К_в = 1 \cdot 72,00 \cdot 1,1 = 79,20 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 5.10.

Таблиця 5.10 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Корпус	1	72,00	79,20
Кнопкова панель	1	64,00	70,40
Гвинти	8	1,50	13,20
Роз’єми	4	12,00	52,80
Трансформатор	1	128,00	140,80
Радіатор	4	85,00	374,00
Діоди	4	15,00	66,00
Операційний підсилювач	11	78,00	943,80
Конденсатори	18	2,80	55,44
Резистори постійні	28	2,90	89,32
Резистори змінні	8	19,20	168,96
Вставка плавка	1	6,50	7,15
Вилка	1	21,00	23,10
Всього			2084,17

5.4.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (5.13)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, (грн.);

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i = *1,10…1,12);*

k – кількість найменувань устаткування.

$$B_{спец} = 11200{,}00 \cdot 1 \cdot 1{,}1 = 12320{,}00 \ (грн.).$$

Отримані результати зведемо до таблиці 5.11.

Таблиця 5.11 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Цифровий генератор	1	11200,00	12320,00
Цифровий осцилограф	1	10560,00	11616,00
Всього			23936,00

5.4.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (5.14)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$$B_{прг} = 4692,00 \cdot 1 \cdot 1,1 = 5161,20 \ (грн.).$$

Отримані результати зведемо до таблиці 5.12.

Таблиця 5.12 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Пакет Visual System Simulator	1	4692,00	5161,20
Пакет Microwave Office	1	3864,00	4250,40
Пакет MATLAB SIMULINK	1	4328,00	4760,80
Всього			14172,40

5.4.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \qquad (5.15)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, (грн.);

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$$A_{обл} = (45799,00 \cdot 1) / (2 \cdot 12) = 1908,29 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 5.13.

Таблиця 5.13 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Програмно-аналітичний комплекс проектування на базі ПК ASUS i5-DJK-0002415	45799,00	2	1	1908,29
Обладнання виводу інформації Лазерний принтер EPSON LaserJet Pro M102w с Wi-Fi (G3Q35A)	6950,00	4	1	144,79
Робоче місце інженера-дослідника спеціалізоване	7840,00	5	1	130,67
Офісна оргтехніка	7899,00	5	1	131,65
Приміщення лабораторії досліджень	642000,00	20	1	2675,00
ОС Windows 11	8380,00	2	1	349,17
Пакет Microsoft Office 2019	7864,00	2	1	327,67
Метрологічний комплекс	13699,00	4	1	285,40
Цифровий генератор	12320,00	5	1	205,33
Цифровий осцилограф	11616,00	5	1	193,60
Всього				6351,56

5.4.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (5.16)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 7,52 (грн.);

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$$B_e = 0,46 \cdot 160,0 \cdot 7,52 \cdot 0,95 / 0,97 = 553,47 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 5.14.

Таблиця 5.14 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Програмно-аналітичний комплекс проектування на базі ПК ASUS i5-DJK-0002415	0,46	160,0	553,47
Обладнання виводу інформації Лазерний принтер EPSON LaserJet Pro M102w с Wi-Fi (G3Q35A)	0,06	10,0	4,51
Робоче місце інженера-дослідника спеціалізоване	0,08	160,0	96,26
Офісна оргтехніка	0,04	5,0	1,50
Метрологічний комплекс	0,12	120,0	108,29

Продовження таблицы 5.14 – Витрати на електроенергію

Цифровий генератор	0,25	120,0	225,60
Цифровий осцилограф	0,75	120,00	676,80
Всього			1666,43

5.4.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \quad (5.17)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 23%.

$$B_{св} = (52016{,}36 + 3418{,}08) \cdot 23 / 100\% = 12749{,}92 \text{ (грн.)}.$$

5.4.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (5.18)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 33%.

$$B_{сп} = (52016,36 + 3418,08) \cdot 33 / 100\% = 18293,37 \text{ (грн.)}.$$

5.4.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.19)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 60%.

$$І_в = (52016,36 + 3418,08) \cdot 60 / 100\% = 33260,67 \text{ (грн.)}.$$

5.4.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків;

витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою

$$B_{нзв} = (З_о + З_р) \cdot \frac{H_{нзв}}{100\%}\ , \qquad (5.20)$$

де $H_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 125%.

$$B_{нзв} = (52016,36 + 3418,08) \cdot 125 / 100\% = 69293,06\ (грн.).$$

Витрати на проведення науково-дослідної роботи на тему «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» розраховуємо як суму всіх попередніх статей витрат за формулою

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \qquad (5.21)$$

$B_{заг}$= 52016,36 +3418,08 +6097,79 +13537,09 +2263,24 +2084,17 +23936,00 + 14172,40 + 6351,56 +1666,43 +12749,92 +18293,37 +33260,67 +69293,06 = =259140,15 (грн.).

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою

$$ЗВ = \frac{B_{заг}}{\eta}, \qquad (5.22)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 259140,15 / 0,9 = 287933,51 (грн.).

5.5 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів пристрою, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, осіб	850	1200	1700	750

N – кількість споживачів які використовували аналогічний пристрій у році до впровадження результатів нової науково-технічної розробки, приймемо 11200 осіб;

$Ц_б$ – вартість пристрою у році до впровадження результатів розробки, приймемо 1280,00 (грн.);

$\pm\Delta Ц_о$ – зміна вартості пристрою від впровадження результатів науково-технічної розробки, приймемо 55,60 (грн.).

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_і$ для кожного із 4-х років, протягом яких очікується отримання позитивних

результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [29]

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (5.23)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо $\rho = 40\%$;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1 = (55,60 \cdot 11200,00 + 1335,60 \cdot 850) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 478592,48$ (грн.).

Збільшення чистого прибутку 2-го року:

$\Delta П_2 = (55,60 \cdot 11200,00 + 1335,60 \cdot 2050) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 914916,97$ (грн.).

Збільшення чистого прибутку 3-го року:

$\Delta П_3 = (55,60 \cdot 11200,00 + 1335,60 \cdot 3750) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 1533043,33$ (грн.).

Збільшення чистого прибутку 4-го року:

$\Delta П_4 = (55,60 \cdot 11200,00 + 1335,60 \cdot 4500) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 1805746,14$ (грн.).

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (5.24)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, (грн.);

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,2;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = 478592{,}48/(1+0{,}2)^1 + 914916{,}97/(1+0{,}2)^2 + 1533043{,}33/(1+0{,}2)^3 +$$
$$+ 1805746{,}14/(1+0{,}2)^4 = 398827{,}06 + 635359{,}01 + 887177{,}85 + 870826{,}65 =$$
$$= 2792190{,}57 \text{ (грн.)}.$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки

$$PV = k_{інв} \cdot ЗВ, \tag{5.25}$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 287933,51 (грн.).

$$PV = k_{інв} \cdot ЗВ = 2 \cdot 287933{,}51 = 575867{,}01 \text{ (грн.)}.$$

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме

$$E_{абс} = ПП - PV \tag{5.26}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 2792190,57 (грн.);

PV – теперішня вартість початкових інвестицій, 575867,01 (грн.).

$$E_{абс} = ПП - PV = 2792190,57 - 575867,01 = 2216323,56 \text{ (грн.)}.$$

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (5.27)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 2216323,56 (грн.);

PV – теперішня вартість початкових інвестицій, 575867,01 (грн.);

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+2216323,56/575867,01)^{1/4} = 0,48.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (5.28)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,1;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,3.

$\tau_{мін}$ = 0,1+0,3 = 0,4 < 0,48 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки

$$T_{ок} = \frac{1}{E_в}, \tag{5.29}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,48 = 2,07 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

5.6 Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» становить 46,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

Значення інтегральної новизни 0,481 – відповідає рівню достатньої новизни; за характеристикою: принципова технологічна модифікація товару;

вид розробки - новий товар, що наділений ознаками інноваційності (інноваційний товар).

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,71 рази.

Також термін окупності становить 2,07 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань».

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

У суспільстві з орієнтацією на соціальну економіку розвиток охорони праці визнається одним із найбільш значущих завдань соціально-економічної політики, не тільки на рівні держави, але й на рівні кожного підприємства та організації. У цьому контексті головним об’єктом охорони праці стає людина, яка піддається впливу небезпечних і шкідливих факторів на виробництві. Основна відповідальність лежить на тих, хто розробляє та впроваджує заходи із захисту від цих факторів, адже процес інтеграції України в Європейське співтовариство передбачає, передусім, зростання уваги до таких аспектів, як безпека людини в різних галузях діяльності.

Під час розробки мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань на працівника, згідно Гігієнічної класифікації праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу, могли мати вплив такі небезпечні та шкідливі виробничі фактори [31]

1. Фізичні: підвищена запиленість та загазованість повітря робочої зони; підвищений рівень шуму на робочому місці; підвищена чи понижена вологість повітря; підвищений рівень електромагнітного випромінювання; підвищена чи понижена іонізація повітря; недостатня освітленість робочої зони; підвищена яскравість світла; понижена контрастність; пряма і відбита блисткість.

2. Психофізіологічні: статичне перевантаження та розумове перевантаження.

Відповідно до наведених факторів здійснюємо розробку заходів щодо безпечного виконання поставленого завдання.

6.1 Технічні рішення щодо безпечного виконання роботи

6.1.1 Обладнання приміщення та робочого місця

Роботодавець має забезпечити, щоб робочі місця відповідали комфортним і безпечним стандартам. Площа одного робочого місця повинна бути не менше 6 м^2. У випадках, коли це необхідно, робочі місця співробітників, які працюють з комп'ютерами, можуть бути розділені перегородками висотою до 2 метрів. При розрахунку відповідного розміру приміщення та робочого місця на одну особу, також враховується наявність шаф, сейфів, тумб чи іншого меблів та обладнання в кімнаті. Площа даного приміщення становить 22,05 м^2, об’єм – 70,56 м^3. в приміщенні працює 3 працівника, тому площа на одну особу становить 7,35 м^2, а об’єм – 23,52 м^3 , що відповідає встановленим вимогам.

На робочому столі працівника можна розмістити додаткові пристрої для роботи, такі як принтери, колонки та сканери, а також забезпечити місце для зберігання документів. Проте важливо впевнитися, що це не обмежує видимість екрану та не заважає працівникам. Робочий стілець працівника повинен бути підйомно-поворотним, з можливістю легкого регулювання висоти, а також здатним забезпечити належну підтримку та комфортне положення для працівника та хребта. Щодня необхідно проводити вологе прибирання приміщення та очищати робоче місце та екран монітора від пилу.

На підприємстві забороняється:

– проводити ремонт та технічне обслуговування комп’ютера за робочим місцем працівника;

– самочинно ремонтувати або намагатись здійснити технічне налагодження комп’ютера без залучення компетентних спеціалістів;

– складати на робочому місці зайві документи, деталі та предмети, що не потрібні для роботи;

– використовувати монітори з нечітким зображенням та монітори, у

яких наявні поламки екрану.

Допускати до роботи осіб, які не пройшли затверджений на підприємстві інструктаж з охорони праці, не дозволяється.

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення праці, так і для підвищення його привабливості та позитивного впливу на продуктивність праці. Правильна робоча поза передбачає наступне:

– стопи повинні розміщуватися на підлозі або на підставці для ніг. Використання підставки є обов'язковим для тих, чиї ноги не досягають підлоги, коли робоче сидіння розташоване на висоті, яка забезпечує оптимальну робочу позицію;

– стегна повинні бути паралельними до підлоги в горизонтальній площині;

– передпліччя має бути розміщені вертикально;

– лікті повинні бути зігнуті під кутом від 70^0 до 90^0 щодо вертикальної площини;

– зап'ястя мають знаходитися під кутом не більше 20^0 відносно горизонтальної площини;

– голову слід тримати під кутом від 15^0 до 20^0 відносно вертикальної площини.

При прийнятті на роботу кожна особа має пройти лікарський огляд. Окрім того, при подальшій трудовій діяльності в компанії, така особа підлягає регулярному лікарському огляду не рідше ніж раз на 2 роки. Обов'язковим є проходження таких лікарів як терапевта, невропатолога та офтальмолога.

У компанії є чітко встановлений графік перерв для відпочинку працівників, окрім обідньої перерви. Зазвичай, ці перерви повинні тривати 10-15 хв і бути надані раз на годину або дві, залежно від характеру та складності роботи. У будь-якому випадку роботодавець має організувати робочий графік на підприємстві таким чином, щоб тривалість неперервної роботи за комп'ютером не перевищувала 4 години. Додатково, для збереження здоров'я

та працездатності, доцільно виділити окреме приміщення для відпочинку працівників та відведення нервово-емоційного напруження, яке виникає під час роботи з комп’ютером.

6.1.2 Електробезпека приміщення

Електробезпека приміщення забезпечується відповідно до ПУЕ. Основними причини ураження працівника в процесі розробки мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань можуть бути [30]^

1. Дотик до металевих неструмоведучих частин (корпусу, периферії комп'ютера), які можуть опинитися під напругою в результаті пошкодження ізоляції.

2. Нерегламентоване використання електричних приладів.

3. Відсутність інструктажу співробітників за правилами електробезпеки.

Для уникнення можливих аварій та замикань, поряд з приміщеннями, де здійснюється робота з комп’ютером (над чи під ними), також не дозволяється проведення робіт, що потребують здійснення надмірно вологих технологічних процесів.

Є неприпустимими:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПУЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Дотримання електробезпеки у приміщенні, де здійснювалася розробка мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань, важливе для запобігання ураженню електричним струмом, що досягається різними способами і заходами:

1. Технічні засоби захисту, такі як ізоляція струмоведучих частин комп'ютерів та периферійних пристроїв, що виключає можливість випадкового дотику до них.

2. Захисне заземлення для металевих неструмоведучих частин, що можуть опинитися під напругою в разі пошкодження ізоляції. Заземлення забезпечує відведення надлишкового струму у землю, запобігаючи ураженню людини.

3. Організаційні заходи, такі як інструктаж і навчання працівників правилам безпеки при роботі з електронікою. Це включає у себе інформування про потенційні ризики та навчання, як уникати їх.

4. Перевірка знань та дотримання правил безпеки, залежно від займаної посади та характеру роботи, є також важливим аспектом організаційних заходів.

6.2 Технічні рішення з гігієни праці та виробничої санітарії

6.2.1 Мікроклімат

Мікроклімат виробничих приміщень впливає на комфорт та працездатність працівників. Параметри мікроклімату, такі як температура повітря, відносна вологість, швидкість руху повітря, важливі для забезпечення оптимальних умов для роботи [32] Підвищена або знижена температура, недостатність вентиляції, висока вологість чи сухе повітря можуть спричинити дискомфорт і негативно впливати на працездатність. Важливо дотримуватися нормативних вимог та створювати оптимальний мікроклімат в приміщеннях, щоб забезпечити комфортні умови для працівників і підтримувати їхню продуктивність.

Мікроклімат виробничих приміщень нормується в залежності від теплових характеристик виробничого приміщення, категорії робіт по важкості і періоду року. Категорія виконуваних робіт під час розробки мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань – 1а (табл.6.1). [32]

Таблиця 6.1 – Параметри мікроклімату

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	21 ... 25 ° С 40 ... 60% до 0,1 м / с
Теплий	Температура повітря в приміщенні Відносна вологість Швидкість руху повітря	22 ... 28 ° С 40 ... 60% 0,1 ... 0,2 м / с

Для підтримання у виробничих приміщеннях необхідних параметрів мікроклімату використовують загальну систему опалення та систему вентиляції. На кожну вентиляційну установку складений паспорт з технічною характеристикою та схемою установки.

6.2.2 Склад повітря робочої зони

Навколишнє повітряне середовище відіграє ключову роль у житті людини і має визначені фізичні та хімічні характеристики, які можуть впливати на здоров’я та комфорт працівників. Фізичні параметри мікроклімату, такі як температура, вологість, швидкість руху повітря і тиск, важливі для підтримки комфортних умов праці. Додатково, іонний склад, електромагнітні та акустичні поля також можуть впливати на самопочуття та працездатність людини.

Забезпечення належних умов мікроклімату та контроль якості повітряного середовища є основними завданнями для забезпечення здоров’я та безпеки на робочому місці. ГДК шкідливих речовин, згідно ДСН 3.3.6.042-99 [33], які можуть знаходитися знаходяться в досліджуваному приміщені, наведені в таблиці 6.2.

Таблиця 6.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Оксид азоту	5	2	3
Вуглекислий газ	3	1	4
Пил нетоксичний	25	10	4
Озон	0,16	0,03	1

Під час роботи на ПК важливо, щоб повітря мало певний іонний склад. Рівні позитивних і негативних іонів у повітрі приміщень з ПК мають відповідати санітарно-гігієнічним нормам (табл.6.3).

Таблиця 6.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 $см^3$	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

Забезпечення складу повітря робочої зони здійснюється за допомогою системи вентиляції, регулярного провітрювання, та вологого прибирання.

6.2.3 Виробниче освітлення

Для забезпечення комфортних умов зорової роботи, попередження швидкої втоми очей, запобігання професійним захворюванням і нещасним випадкам, а також для підвищення продуктивності праці важливо, щоб виробниче освітлення відповідало наступним критеріям: забезпечення на робочій поверхні необхідного рівня освітленості, який відповідає характеру зорової роботи та не опускається нижче встановлених норм; уникнення засліплюючої дії як від самого джерела освітлення, так і від інших об’єктів, що потрапляють у поле зору; збереження сталого та рівномірного рівня освітленості виробничих приміщень, щоб уникнути постійного переадаптування очей; попередження виникнення глибоких і різких тіней на робочій поверхні, особливо тих, що можуть змінюватися під час роботи; забезпечення достатнього контрасту між освітленою поверхнею та робочим об’єктом для зручного розрізнення деталей; забезпечення надійності та простоти обслуговування системи освітлення, а також врахування економічних і естетичних аспектів.

Норми освітленості при штучному освітленні та КПО при природному та сумісному освітленні (характеристика зорової роботи – дуже високої точності

згідно з ДБН В.2.5-28:2018 [34] «Природне і штучне освітлення») зазначені у таблиці 6.4:

Таблиця 6.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$,%			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Високої точності	0,3 - 0,5	III	г	великий	світлий	700	300	5	2	3	1,2

Для оптимізації використання природного освітлення в приміщенні необхідно систематично очищати вікна від пилу та встановити жалюзі. Важливо також переконатися, що віконні прорізи не затемнюються будь-якими іншими будівлями чи об’єктами, що можуть перекривати світло.

Як джерела світла для штучного освітлення в приміщенні використовують люмінесцентні лампи. Важливо, щоб світильники були розташовані ефективно та рівномірно, щоб забезпечити оптимальну освітленість на робочих поверхнях та у всьому приміщенні.

6.2.4 Виробничий шум

Шум є фактором, який впливає на організм людини не лише шляхом безпосереднього подразнення слухового апарату, але також через вплив на центральну нервову систему. Це може призводити до різних порушень в роботі різних систем організму. Ефекти впливу шуму на організм людини можна

умовно поділити на дві групи: специфічні, пов’язані з впливом шуму на органи слуху, і загальні (неспецифічні), які виникають в різних органах і системах організму, крім слухового апарату. Основним джерелом шуму в приміщенні, де проводиться розробка мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань є працююча офісна техніка. Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ПК, мають відповідати вимогам ДСН 3.3.6.037-99 35 (табл.6.5).

Таблиця 6.5 - Рівень звукового тиску

Характер робіт	Допустимі рівні звукового тиску (дБ) в								
	32	63	125	250	500	1000	2000	4000	8000
Постійні робочі місця в промислових .	107	95	87	82	78	75	73	71	69

На робочому місці рівень шуму є нижчим за нормований. При появі значного рівня шуму доцільним є використання шумоізолюючих матеріалів в інтер'єрі (меблі та обробка приміщень звукоізоляційними матеріалами можуть допомогти знизити внутрішні відбиття звуку), оптимізація розташування робочих місць (віддалено від джерел шуму або використання перегородок для виділення тих зон, де шум може бути більшим), а також дотримання раціонального режиму праці та відпочинку.

6.2.5 Виробничі випромінювання

Джерелами змінних електричних і магнітних полів у комп’ютері є компоненти у яких присутні високі змінна напруга та великі струми. Рівні електромагнітних полів визначаються за електричними параметрами та магнітною індукцією і регулюються чинними нормами України, зокрема Державним санітарними правилами та нормами ДСанПіН 3.3.2.007-98 [36], а

також європейським стандартом MPR II, відомим як «шведський стандарт». Також ці діапазони розглядаються в універсальному рекомендаційному стандарті ТСО'99. У разі некоректної організації живлення робочого місця джерелами електричних і магнітних полів можуть бути не лише монітор комп'ютера, блок живлення системної одиниці та мережеві кабелі, але й периферійні пристрої.

Значення напруженості електростатичного поля на робочих місцях із ПК (як у зоні екрана дисплея, так і на поверхнях обладнання, клавіатури, друкувального пристрою) мають не перевищувати гранично допустимих (табл.6.6). [38]

Таблиця 6.6 – Допустимі параметри електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні відеомонітору	10 В/м
Напруженість магнітної складової електромагнітного я на відстані 50 см від поверхні відеомонітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати:	для дорослих користувачів 20кВ/м для дітей 15кВ/м

Для забезпечення захисту і досягнення нормованих рівнів комп'ютерних випромінювань необхідно застосовувати засоби індивідуального захисту очей та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат. Для зменшення впливу ЕМП на працівника необхідно дотримуватися раціонального режиму роботи та відпочинку, встановленого нормативними вимогами.

6.2.6 Психофізіологічні фактори

Оцінка психофізіологічних факторів під час розробки мікроелектронного пристрою для технічного захисту інформації з використанням генератора

хаотичних коливань здійснюється відповідно до Гігієнічної класифікацією праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу [39].

Робоча поза: періодичне перебування в незручній позі (робота з поворотом тулуба, незручним розташуванням кінцівок) та/або фіксованій позі (неможливість зміни взаєморозташування різних частин тіла відносно одна одної) до 25% часу зміни;

Класи умов праці за показниками напруженості праці:

Інтелектуальні навантаження:

Зміст роботи – творча діяльність, що вимагає вирішення складних завдань за відсутності алгоритму;.

Сприймання інформації та їх оцінка – сприймання інформації з наступною корекцією дій та операцій;

Розподіл функцій за ступенем складності завдання – обробка, виконання завдання та його перевірка.

Сенсорні навантаження:

Зосередження (%за зміну) – до 5-75%;

Щільність сигналів (звукові за1 год) – до 150;

Навантаження на слуховий аналізатор (%) – розбірливість слів та сигналів від 50 до 80 %;

Спостереження за екранами відеотерміналів (годин на зміну) – 4-6год.

Навантаження на голосовий апарат (протягом тижня) – від 16 до 20.

Емоційне навантаження:

Ступінь відповідальності за результат своєї діяльності – є відповідальним за функціональну якість основної роботи; Ступінь ризику для власного життя – вірогідний;

Режим праці:

Тривалість робочого дня – більше 8 год;

Змінність роботи – однозмінна (без нічної зміни).

За зазначеними показниками важкості та напруженості праці, робота, яка виконується належить до допустимого класу умов праці (напруженість праці середнього ступеня).

6.3 Безпека в надзвичайних ситуаціях. Дослідження безпеки роботи РЕС мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань в умовах дії загрозливих факторів НС

6.3.1 Дія електромагнітних випромінювань на радіоелектронні системи

Електромагнітний імпульс (ЕМІ) як уражаючий фактор здатний розповсюджуватись на десятки і сотні кілометрів лініями електропередач, зв'язку, трубопроводах. Особливо піддаються ЕМІ радіоелектронна апаратура, системи автоматичного управління. ЕМІ також пробиває ізоляцію, випалює елементи електронних схем, викликає коротке замикання, стирає магнітний запис ЕОМ.

Електромагнітний імпульс може вивести з ладу електронну систему управління, дати збої у роботі, спричинити аварії та нещасні випадки, в результаті яких можуть загинути люди.

До матеріалів, з яких виготовляють елементи радіоелектронних систем (РЕС) відносять: метали, неорганічні матеріали, напівпровідники та різні органічні сполуки (діелектрики, смоли тощо).

З метою запобігання цього проводяться розрахунки з безпеки роботи в умовах дії електромагнітних випромінювань та приймаються рішення щодо захисту елементів РЕС [41].

6.3.2 Оцінка безпеки роботи РЕС мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань в умовах дії електромагнітних випромінювань

Вихідні дані: $U_Ж = 5 \pm 5\%$ В; $l_Г = 0$ м; $l_В = 0{,}05$ м.

$l_Г = 0$ м, оскільки усі струмоведучі частини РЕС даного приладу розташовані у вертикальній площині.

За критерій стійкості РЕС в умовах дії електромагнітного імпульсу приймається коефіцієнт безпеки, який визначається за формулою [5.1]

$$K_Г = 20\lg\frac{U_Д}{U_В} \geq 40 \text{ [дБ].} \tag{6.1}$$

Знаходимо допустиме коливання напруги живлення

$$U_Д = U_Ж + \frac{U_Ж}{100}N \text{ [В];} \tag{6.2}$$

$$U_Д = 5 + \frac{5}{100}5 = 5{,}25 \text{ (В),}$$

де $U_Ж$ – робоча напруга живлення, В;

N – допустимі коливання напруги, %.

З формули (6.1) виразимо вертикальну складову напруги наведення на струмопровідних частинах РЕС

$$U_В = \frac{U_Д}{100} \text{ [В];} \tag{6.3}$$

$$U_В = \frac{5{,}25}{100} = 0{,}05 \text{ (В).}$$

Знаходимо допустиму горизонтальну складову напруженості електромагнітного поля, при якому коефіцієнт безпеки знаходиться в межах допустимого

$$U_B = E_Г l_B \text{ [В]}, \tag{6.4}$$

звідки

$$E_Г = \frac{U_B}{l_B} \text{ [В/м]}; \tag{6.5}$$

$$E_Г = \frac{0{,}05}{0{,}05} = 1 \text{ (В/м)}.$$

Знаходимо допустиму вертикальну складову напруженості електромагнітного поля, при якому коефіцієнт безпеки знаходиться в межах допустимого

$$E_Г = 10^{-3} E_B \text{ [В/м]}, \tag{6.6}$$

звідки

$$E_B = \frac{E_Г}{10^{-3}} \text{ [В/м]}; \tag{6.7}$$

$$E_B = \frac{1}{10^{-3}} = 1000 \text{ (В/м)} = 1 \text{ (кВ/м)}.$$

6.4 Висновки

Отже, знайдено допустимі горизонтальну та вертикальну складові напруженості електромагнітного поля, при яких коефіцієнт безпеки знаходиться в межах допустимого, тобто забезпечується безпечна робота РЕС мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань в умовах дії електромагнітних випромінювань.

ВИСНОВКИ

В магістерській кваліфікаційній роботі проводились дослідження генератора хаотичних коливань для захисту інформації. Проведено літературний огляд поставленого питання, аналіз існуючих аналогів та обґрунтовано актуальність обраної теми.

В першому розділі роглянуто основні системи шифрування, класифікацію шифрів за різними ознаками та здійснено аналіз їх математичних моделей. Також було роглянуто питання основних властивостей динамічних хаотичних систем на основі чого було виокремлено основні вимоги до хаотичних алгоритмів шифрування.

В другому розділі було роглянуто основне поняття хаосу, його властивості та особливості, найвідоміші на сьогоднішній день алгоритми передачі інформації із застосуванням хаосу, також досліджено схему Чуа. В ході дослідження було отримані вихідні сигнали на виході генератора, спектр сигналу, а також фазові портрети аттрактора при різних значеннях опору. Отримали аттрактор типу «подвійний виток».

В третьому розділі в ході виконання комп'ютерного моделювання було досліджено генератор хаотичних коливань та його властивості. Були отримані вихідні сигнали на виході генератора, спектр сигналу, а також фазові портрети аттрактора при різних значеннях опору. Досліджено, що зменшуючи значення опору R_8 призводить до того, що точка перетворюється на орбіту. Подальше зменшення опору призвело до роздвоювання цієї орбіти, спостерігалися біфуркації типу «подвійний виток».

В четвертому розділі досліджено систему захисту інформації, що експериментально реалізована на операційних підсилювачах і помножувачах сигналів. Отримані часові діаграми та спектри сигналу показали, що вихідний сигнал на приймальній стороні збігається з вхідним інформаційним сигналом, що свідчить про захисні властивості даної системи.

В розділі економіки гідно проведених досліджень рівень комерційного потенціалу розробки за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань» становить 46,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий). Таким чином, це свідчить про те що, що генератори хаосу, побудовані на вирішенні рівнянь динамічних систем, успішно можуть використовуватися для захисту інформації.

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,71 рази.

Також термін окупності становить 2,07 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань».

В розділі охорони праці та безпеки надзвичайних ситуацій, знайдено допустимі горизонтальну та вертикальну складові напруженості електромагнітного поля, при яких коефіцієнт безпеки знаходиться в межах допустимого, тобто забезпечується безпечна робота РЕС мікроелектронного пристрою для технічного захисту інформації з використанням генератора хаотичних коливань в умовах дії електромагнітних випромінювань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дідковський Р. М. Теоретичне та експериментальне дослідження завадостійкості системи на основі кореляційної хаотичної модуляції з додаванням ортогоналізованої затриманої компоненти / Р. М. Дідковський, С. С. Гузнін // Вісник Хмельницького національного університету. – 2010. – № 1. – С. 280–286.

2. Kocarev L. Chaos-based cryptography: A brief overview / L. Kocarev.- : IEEE Circuit and Systems Magazine. 2001.- 6 pp.

3. Brown R. Clarifying chaos: examples and counterexamples / R. Brown, L. Chua. -Int. J. Bifurcation and Chaos, 2000. – 219 pp.

4. Oseledec V.I. A multiplicative ergodic theorem: Lyapunov characteristic numbers for dynamical systems / V.I. Oseledec - Trans. Mosc. Math. Soc. 1968. V. 19. № 197.

5. Andreyev Yu. A Cryptosystem based on chaotic dynamics / Yu Andreyev, A.A. Dmitriev - Proceedings SCS'2001. Iasi. Romania, 2001. - 57 pp.

6. Dmitriev A.S Chaotic synchronization. Information viewpoint / A.S. Dmitriev, G.A Kassian, A.D. Khilinsky; int. J. Bif. Chaos., 2000. - V. 10. № 2, 749 pp.

7. Матвійчук Я. М. Математичне моделювання хаотичних рухів у детермінованих системах / Я.М. Матвійчук. – Львів: Вісн. Львів. ун-ту, 1993.- 61-66, [6] с. – (Сер. фіз.).

8. Матвійчук Я. М. Електрична та математичні реалізації схеми Чуа / Я.М. Матвійчук, М.В. Хараба.- Теор. електротехніка., 1994.- 169-179 [52] с.

9. A.S. Elwakil, and M.P. Kennedy, “Chua's circuit decomposition: a systematic design approach for chaotic oscillators,” Journal of the Franklin Institute, No 337, 2000, pp. 251-265.

10. A. S. Elwakil and M. P. Kennedy, “Improved Implementation of Chua's Chaotic Oscillator Using Current Feedback Op Amp,” IEEE Transactions On Circuits And Systems, Part 1, Vol. 47, No. 1, pp. 76-79, January 2000.

11. J. M. Munoz-Pacheco, and E. Tlelo-Cuautle, “Automatic synthesis of 2D-n-scrolls chaotic systems by behavioral modeling,” Journal of Applied Research and Technology, Vol.7 No. 1, April 2009, pp. 5-14.

12. E. Tamaseviciute, A. Tamasevicius, G. Mykolaitis, S. Bumeliene, and E. Lindberg, “Analogue Electrical Circuit for Simulation of the Duffing-Holmes Equation,” Nonlinear Analysis: Modelling and Control, Vol. 13, No. 2, 2008, pp. 241–252.

13. Zdenek HRUBOS, “Novel circuit implementation of universal and fully analog chaotic oscillator,” PRZEGLA˛D ELEKTROTECHNICZNY (Electrical Review), R. 88 NR 7a/2012, pp. 18-22.

14. Jiři PETRŽELA, Zdeněk KOLKA, and Stanislav HANUS, “Simple Chaotic Oscillator: From Mathematical Model to Practical Experiment,” RADIOENGINEERING, VOL. 15, NO. 1, pp. 6-12, APRIL 2006.

15. Jiri PETRZELA, and Tomas GOTTHANS, “Chaotic oscillators with single polynomial nonlinearity and digital sampled dynamics,” PRZEGLĄD ELEKTROTECHNICZNY (Electrical Review), R. 87 NR 6/2011, pp. 161-163.

16. Qais H. Alsafasfeh, and Mohammad S. Al-Arni, “A New Chaotic Behavior from Lorenz and Rossler Systems and Its Electronic Circuit Implementa,” Circuits and Systems, 2, 2011, pp. 101-105.

17. Ihsan Pehlivan, and Yılmaz Uyaroglu, “A new chaotic attractor from general Lorenz system family and its electronic experimental implementation,” Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010, pp. 171-184.

18. Ndombou GB, Marquie P, Fomethe A3, Yemele D, Jeutho MG3 and Kenmogne F, “Chaotic Pulse Generation Induced by a Specific Class of Autonomous Oscillator,” Journal of Electrical & Electronic Systems, Volume 5 • Issue 2, pp. 1000181 1-7.

19. Ihsan Pehlivan, Yilmaz Uyaroglu, and Mesut Yogun, “Chaotic oscillator design and realizations of the Rucklidge attractor and its synchronization and masking simulations,” Scientific Research and Essays Vol. 5(16), pp. 2210-2219, 18 August, 2010, pp. 2210-2219.

20. A.S. Elwakil, and M.P. Kennedy, “A low-voltage, low-power, chaotic oscillator, derived from a relaxation oscillator,” Microelectronics Journal No 31 (2000), pp. 459–468.

21. A. Ferikoğlu, Ya. Sarı, and R. Koker, “Design and Analysis of Negative Value Circuit Components in PSpice Simulation Software,” Computer Modelling and New Technologies, 2013, vol. 17, No. 2, pp. 53–59.

22. Van Ha Nguyen, and Han Jung Song, “Bifurcation Analysis of the Voltage Controlled Photosensitive Chaotic Oscillator,” CHIN. PHYS. LETT. Vol. 30, No. 6 (2013), pp. 060501 1-4.

23. Han Jung Song, and John G. Harris, “A CMOS Neural Oscillator Using Negative Resistance,” Proceedings Of The 2003 IEEE International Symposium On Circuits And systems, 25-28 May 2003, pp. III-152 - III-155.

24. Buncha Munmuangsaen and Banlue Srisuchinwong, “Chaos in Modified CFOA-Based Inductorless Sinusoidal Oscillators Using a Diode,” Chaotic Modeling and Simulation (CMSIM) No 1, pp. 179-185, 2013.

25. A. Semenov, A. Savytskyi, O. Semenova, and M. Huz, “Numerical Simulation of the Chua’s Oscillator Based on a MOSFET Structure with a Cubic Nonlinearity,” 2018 9th International Conference on Ultrawideband and Ultrashort Impulse Signals (UWBUSIS). IEEE, Sep. 2018. doi: 10.1109/uwbusis.2018.8520001.

26. A. Semenov, O. Osadchuk, O. Semenova, O. Bisikalo, O. Vasilevskyi, and O. Voznyak, “Signal Statistic and Informational Parameters of Deterministic Chaos Transistor Oscillators for Infocommunication Systems,” 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). IEEE, Oct. 2018. doi: 10.1109/infocommst.2018.8632046.

27. A. Semenov, “Numerical researching the radiofrequency Chua’s oscillator based on a device with negative differential resistance,” 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). IEEE, Sep. 2017. doi: 10.1109/ukrmico.2017.8095376.

28. A. Semenov, “Radiofrequency deterministic chaos oscillator based on a transistor structure with negative resistance. Numerical researching,” 2017 XI

International Conference on Antenna Theory and Techniques (ICATT). IEEE, May 2017. doi: 10.1109/icatt.2017.7972659.

29. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

30. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа – Вінниця : ВНТУ, 2016. – 113 с.

31. Наказ від 08.04.2014 № 248 Про затвердження Державних санітарних норм та правил Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/topiccatalogua/labor-protection/14._nakazy_ta_rozpor_183575/248+58074-detail.html

32. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. - [Електронний ресурс] - Режим доступу: http://sop.zp.ua/norm_npaop_0_00-7_15-18_01_ua.php

33. ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги - [Електронний ресурс] - http://online.budstandart.com/ua/catalog/doc-page?id_doc=71028

34. ДСан ПіН 3.3.2.007-98 Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ЕОМ - [Електронний ресурс] - Режим доступу: http://document.ua/derz-nor4881.html

35. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

36. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. [Електронний ресурс] – Режим доступу до сторінки: http://hrliga.com/index.php?module=norm_base&op=view&id=819

37. Правила улаштування електроустановок - [Електронний ресурс] - Режим доступу: http://www.energiy.com.ua/PUE.html

38. СанПіН 2.2.4.1294-03 «Фізичні фактори виробничого середовища. Гігієнічні вимоги до аероіонного складу повітря виробничих і громадських приміщень» - [Електронний ресурс] - Режим доступу: http://www.ionization.ru/issue/iss5.htm

39. СанПіН 2.2.4.1191-03 «Електромагнітні поля у виробничих умовах» - [Електронний ресурс] - Режим доступу: http://www.vrednost.ru/2241191-03.php

40. ДБН В.2.5-28:2018 Природне і штучне освітлення - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=79885

41. Методичні вказівки до самостійної та індивідуальної роботи з дисципліни "Цивільний захист та охорона праці в галузі. Частина 1. Цивільний захист" / Уклад. О. В. Поліщук, О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2017. – 32 с.

Додаток А

(обов`язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

МІКРОЕЛЕКТРОННИЙ ПРИСТРІЙ ДЛЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ

Виконав: студент 2-го курсу, групи МНТ-22м спеціальності 153 «Мікро- та наносистемна техніка»
(шифр і назва напряму підготовки, спеціальності)
_____ Штефанеса С.С.
(прізвище та ініціали)

Керівник: д.т.н., проф., проф. каф. ІРТС
_____ Семенов А.О.
(прізвище та ініціали)
«18» 12 2023 р.

Вінниця ВНТУ - 2023 рік

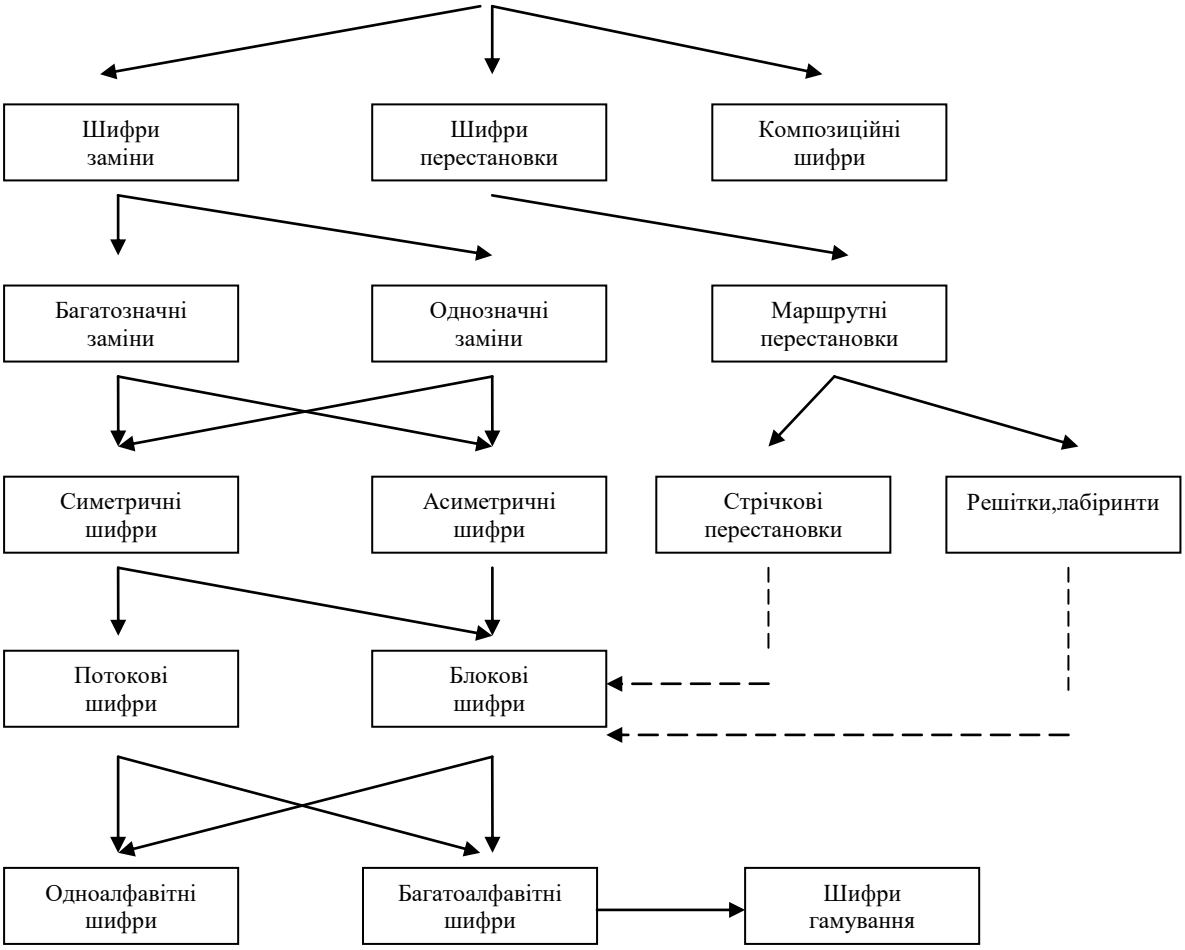


Рисунок 1 – Класифікація шифрів

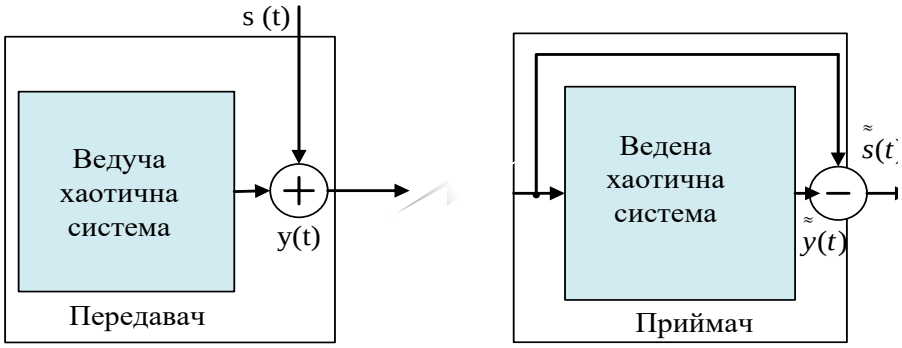


Рисунок 2 – Хаотичне маскування

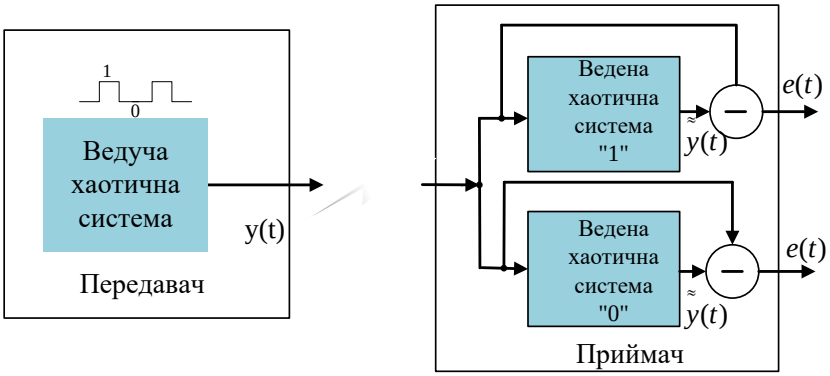


Рисунок 3 – Перемикання хаотичних режимів

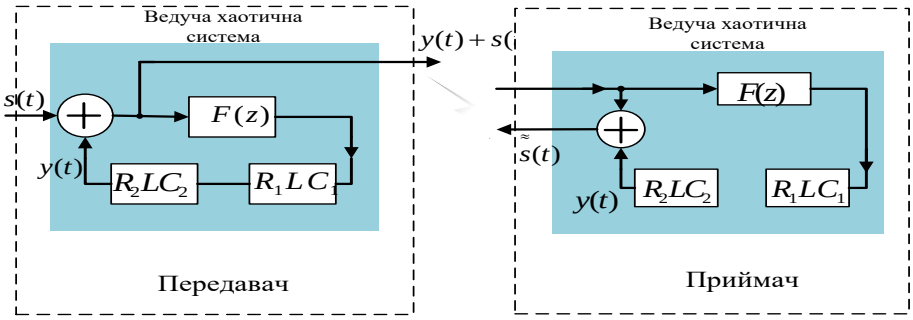


Рисунок 4 – Нелінійне підмішування сигналів

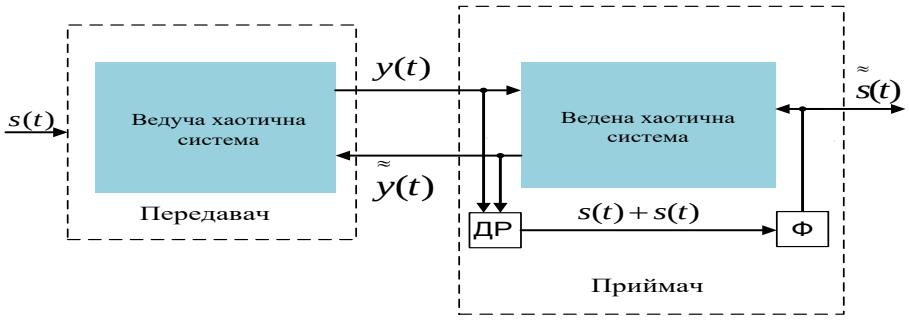


Рисунок 5 – Рознесення сигналів

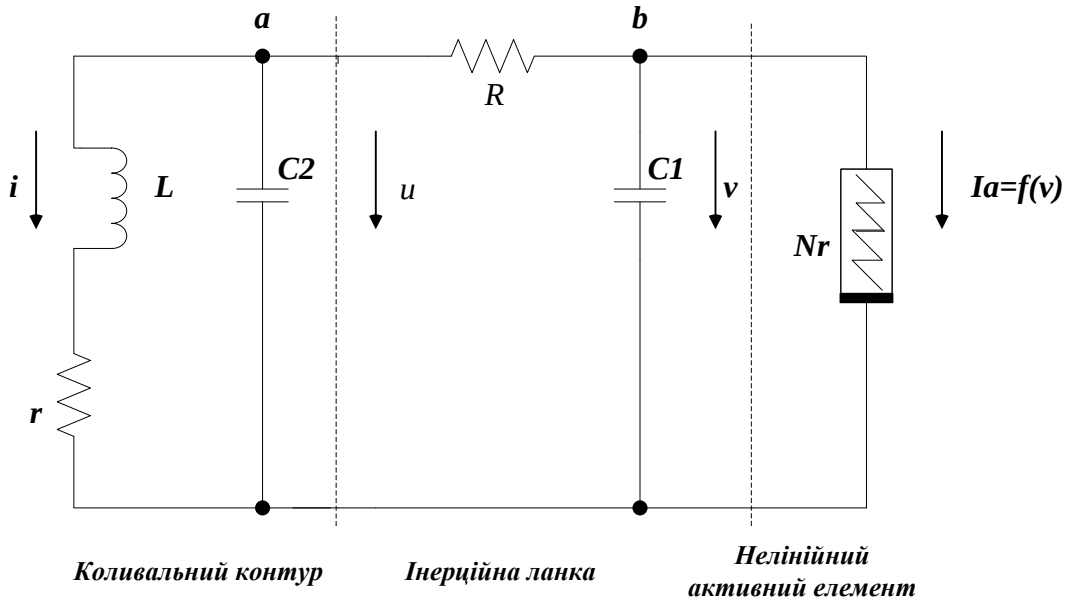


Рисунок 6 – Схема генератора Чуа

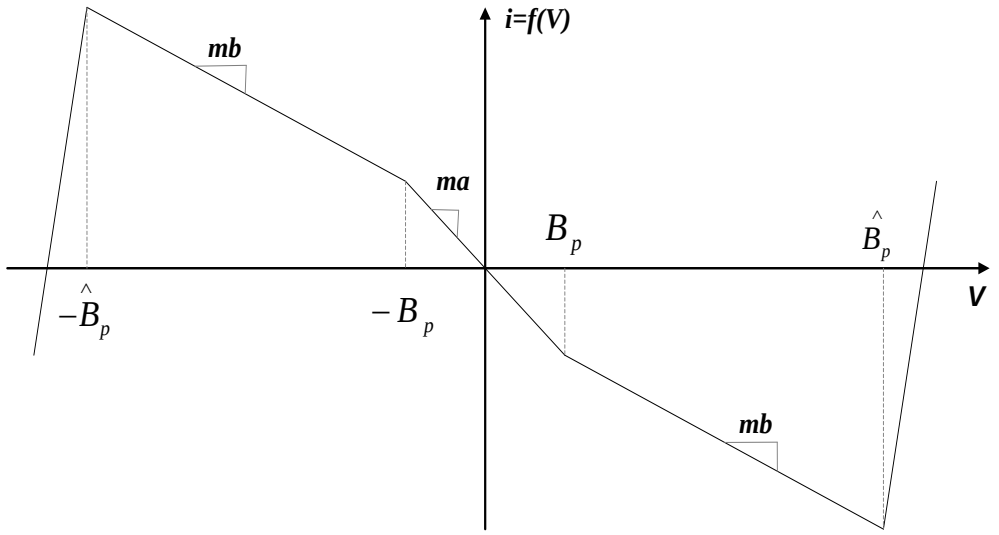


Рисунок 7 – Вольт-амперна характеристика нелінійного елемента

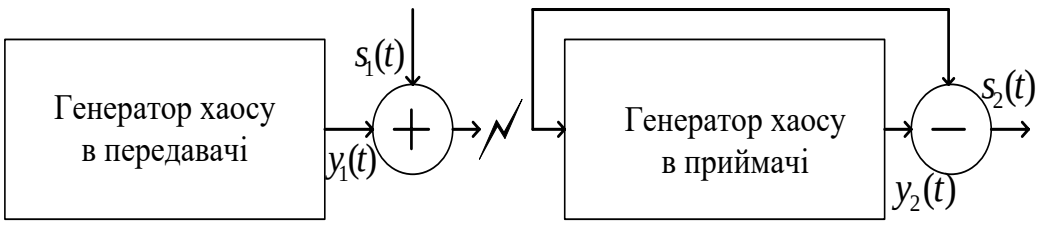


Рисунок 8 - Схема маскування хаотичним сигналом

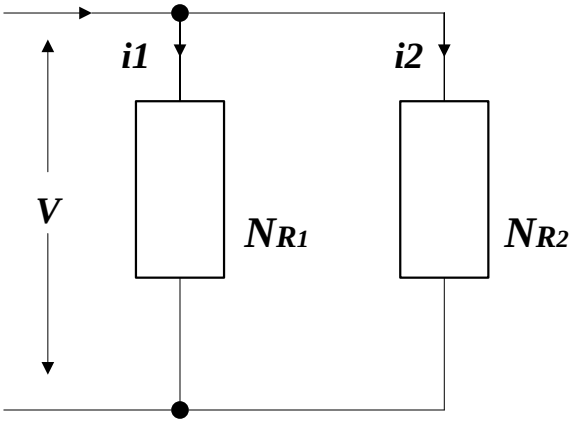


Рисунок 9 – Паралельне з’єднання двох кусково-лінійних резисторів

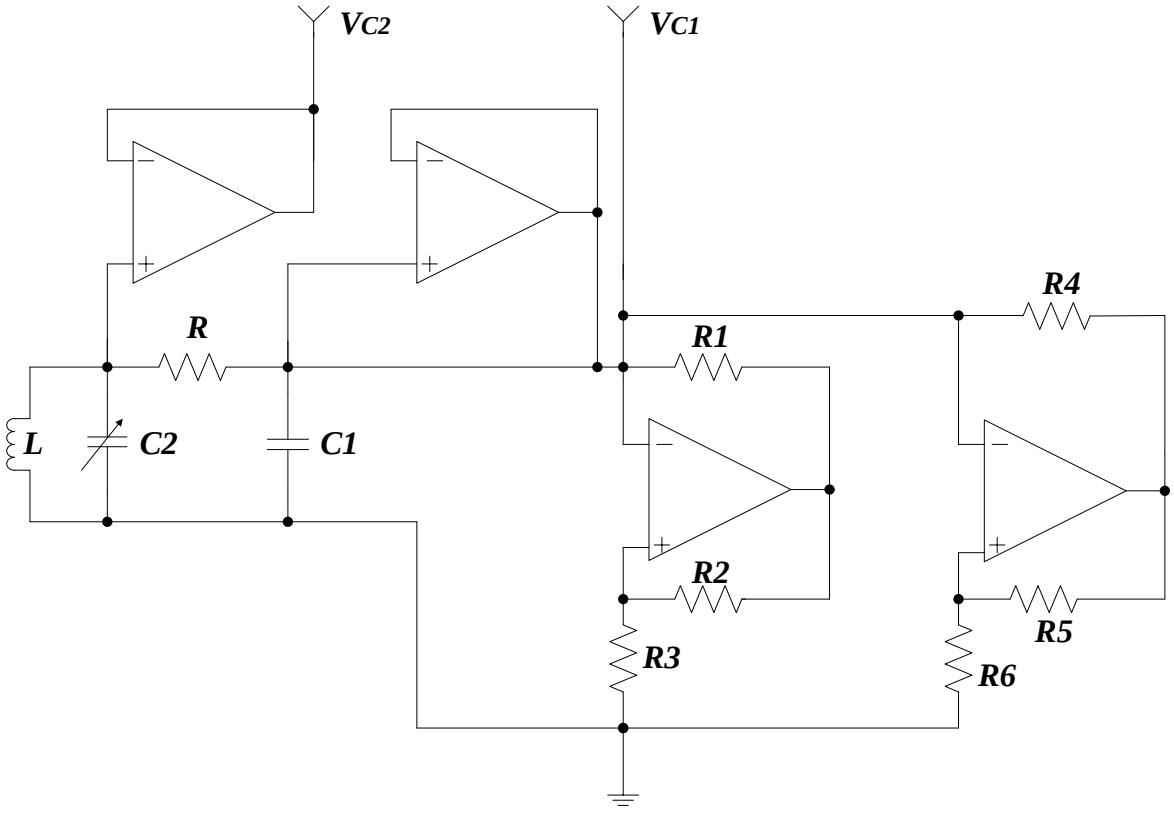


Рисунок 10 – Принципова схема системи Чуа. Додаткові ОП включені в схему для усунення впливу вимірювальних приладів на динаміку системи Чуа

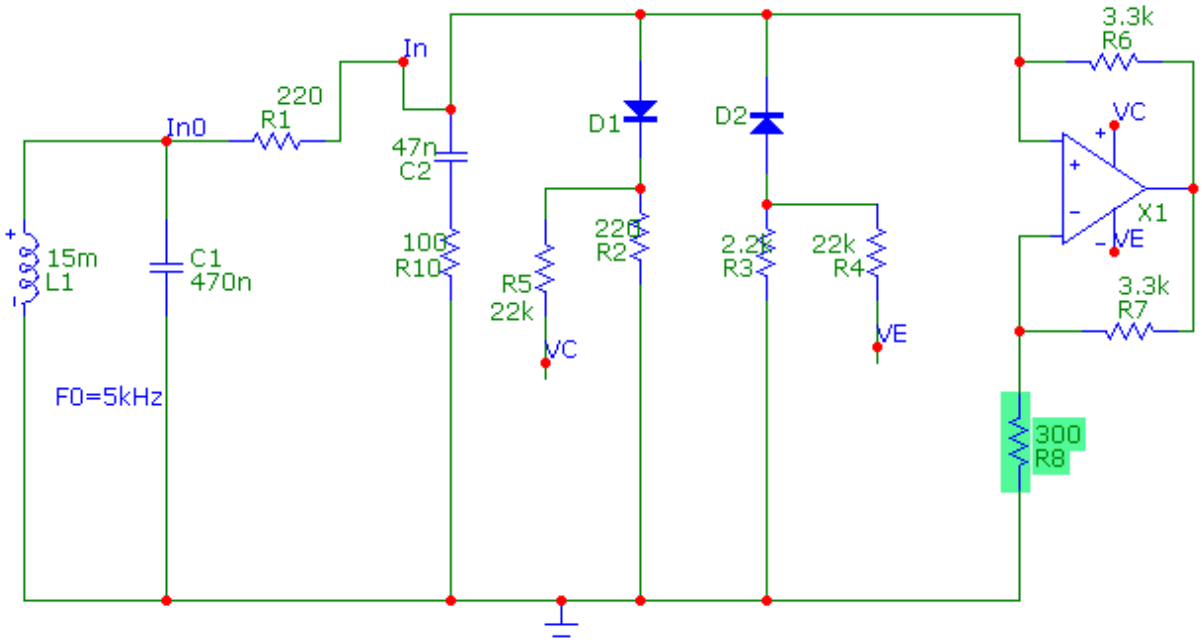


Рисунок 11 - Реалізація схеми генератора Чуа в програмному пакеті Micro-Cap

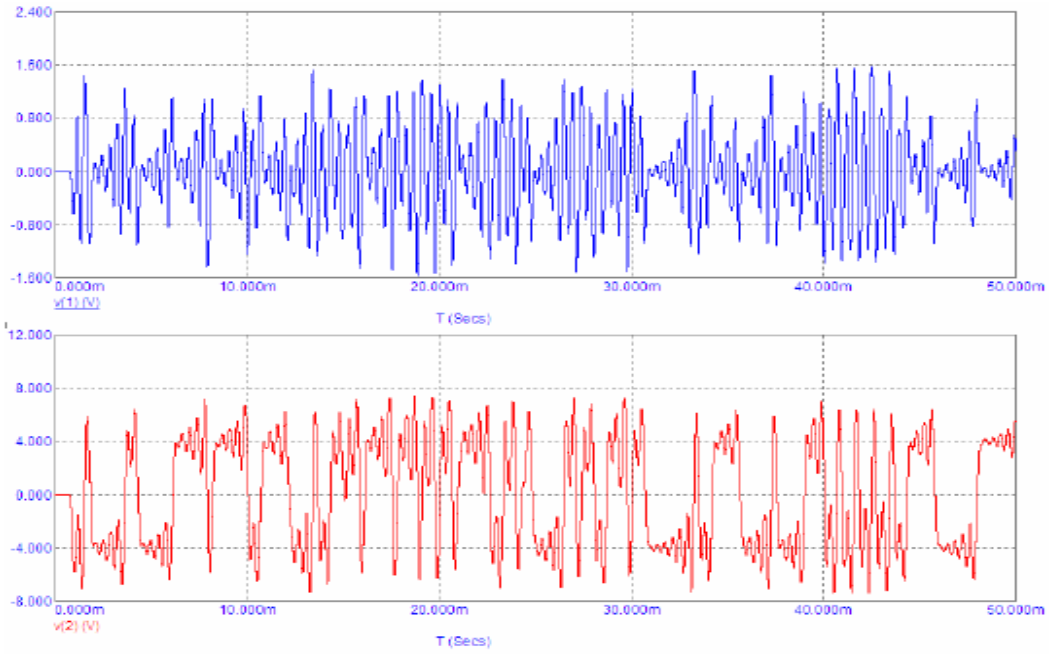


Рисунок 12 – Часова діаграма сигналу на виході генератора

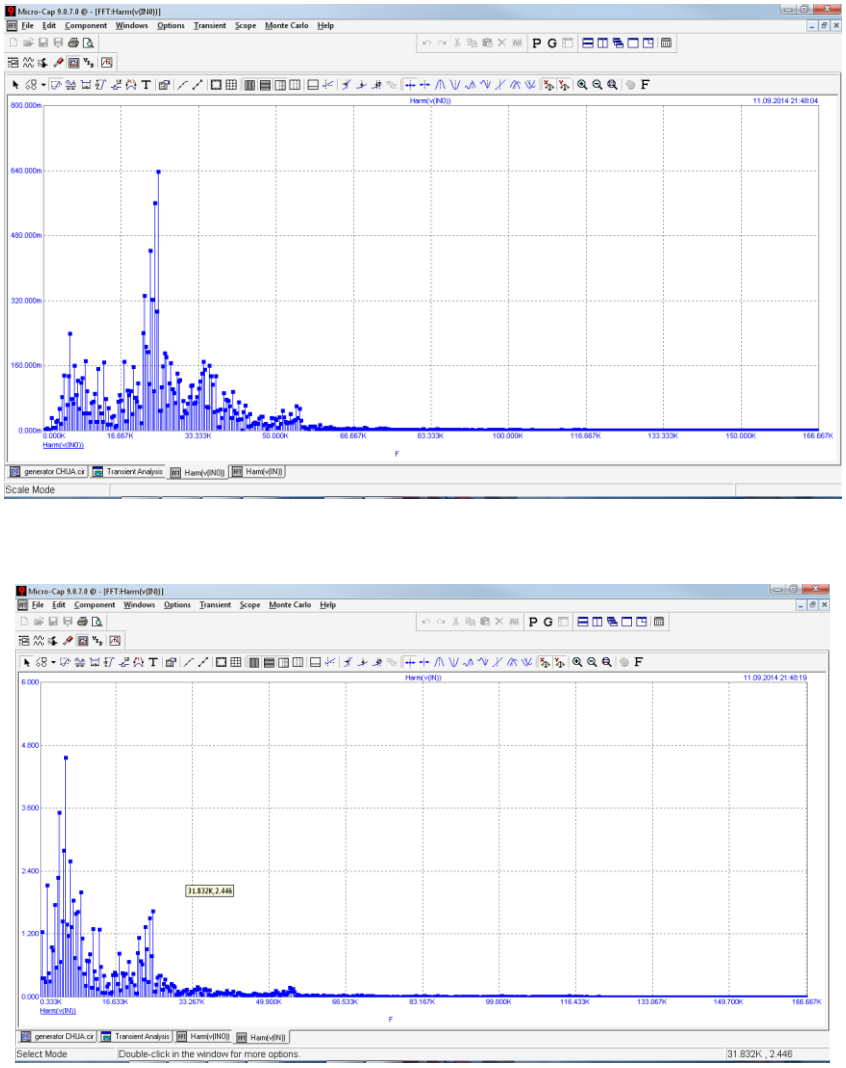


Рисунок 13 - Спектральні характеристики генерованих схемою Чуа сигналів

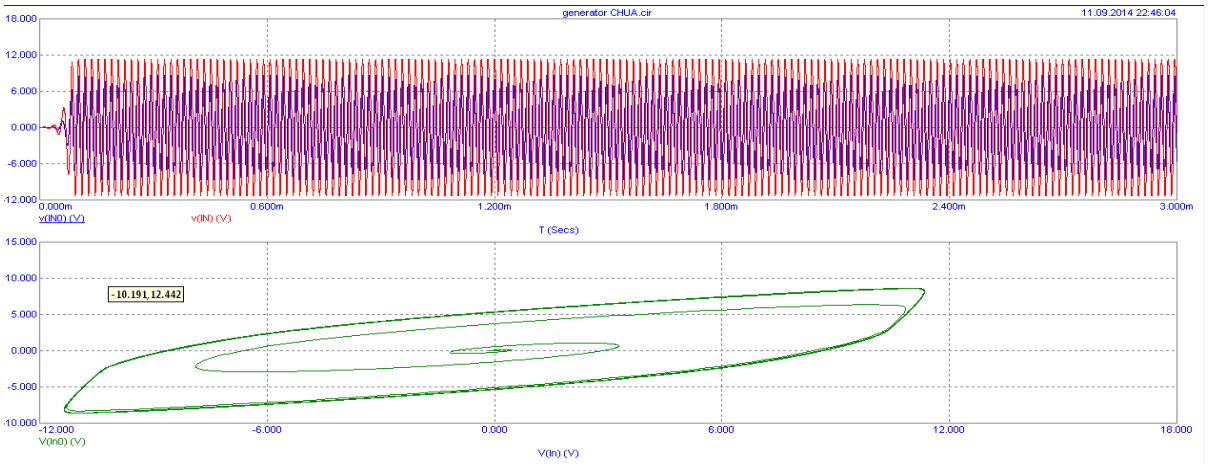


Рисунок 14 – Сигнал на виході генератора хаосу та його фазовий портрет

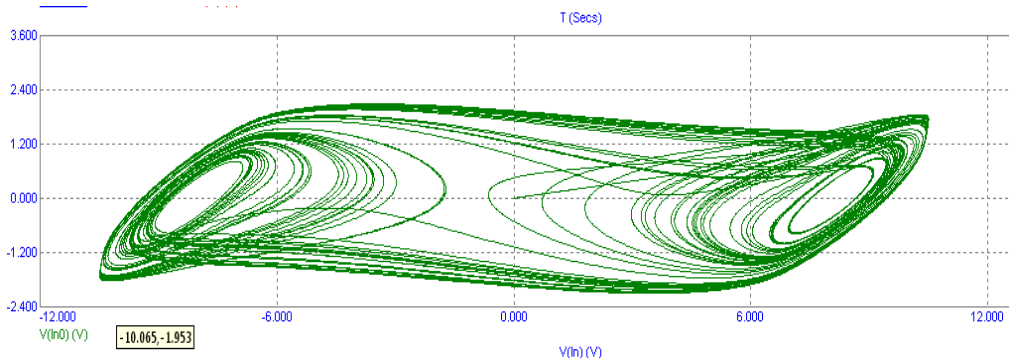


Рисунок 15 – Фазовий портрет аттрактора «подвійний виток»

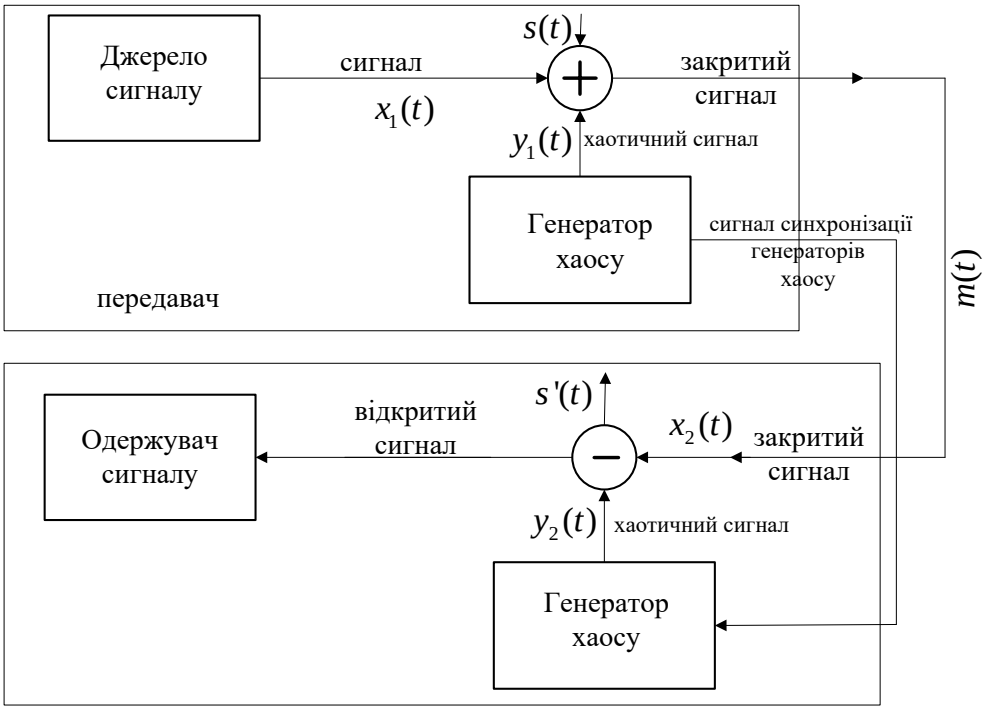


Рисунок 16 – Структурна схема генератора хаосу

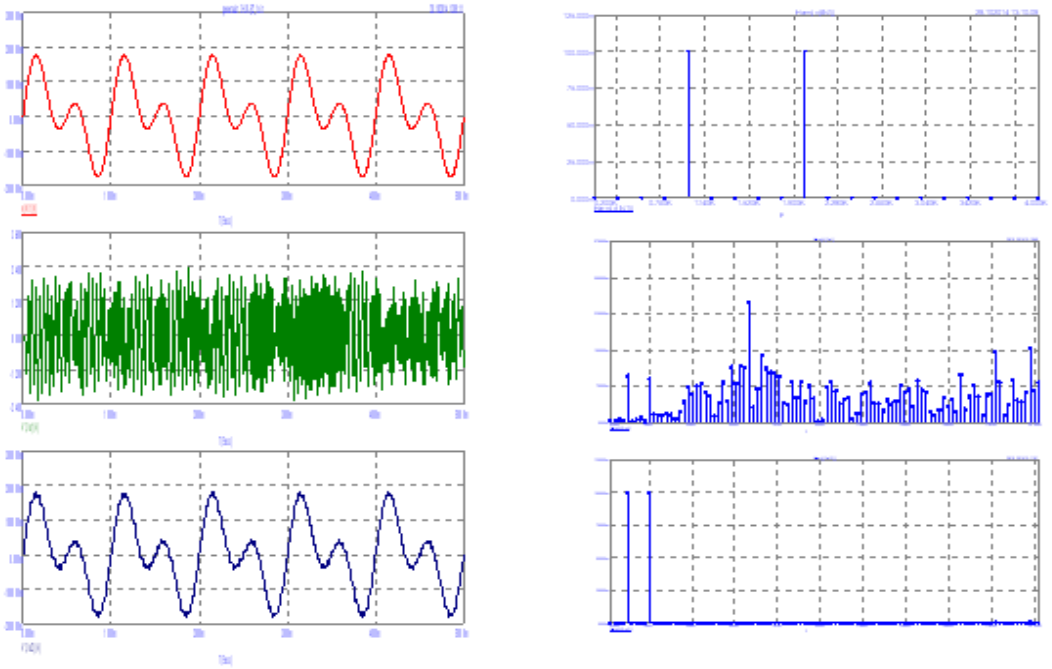


Рисунок 17 – Часові діаграми та спектри сигналів: а) вхідного інформаційного сигналу; б) закритого сигналу; в) розшифрованого сигналу (правильно)

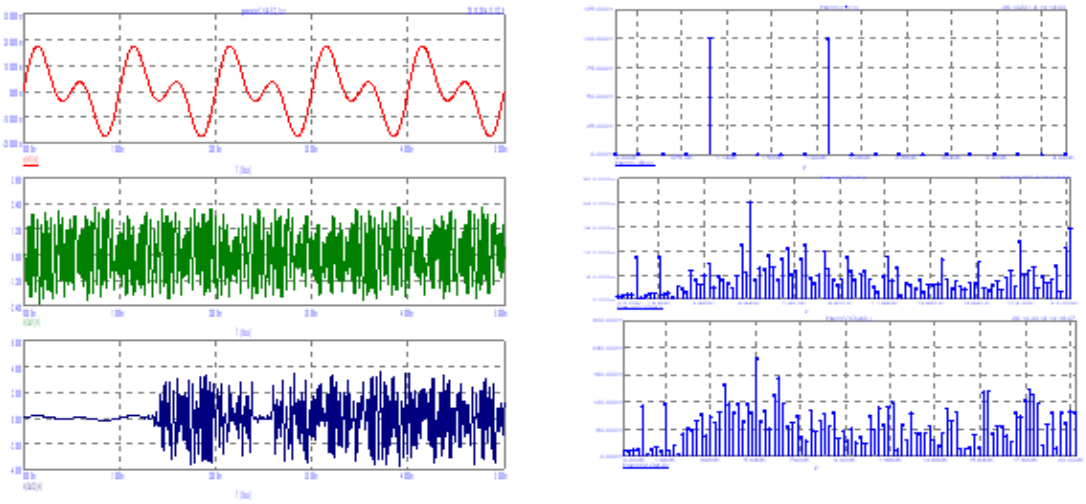


Рисунок 18 – Часові діаграми та спектри сигналів: а) вхідного інформаційного сигналу; б) закритого сигналу; в) розшифрованого сигналу (неправильно)

Додаток Б

(обов`язковий)

ПРОТОКОЛ ПЕРЕВІРКИ РОБОТИ

МІКРОЕЛЕКТРОННИЙ ПРИСТРІЙ ДЛЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ГЕНЕРАТОРА ХАОТИЧНИХ КОЛИВАНЬ

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: «Мікроелектронний пристрій для технічного захисту інформації з використанням генератора хаотичних коливань»

Тип роботи: Магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра ІРТС
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 84,9% Схожість 15,1%

Аналіз звіту подібності (відмітити потрібне):

☑ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Звягін О.С.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Штефанеса С.С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Семенов А.О.
(підпис) (прізвище, ініціали)