УДК 621.391 **О.В. Гресь, А.Д. Верига, Р.Л. Політанський, О.В. Дробик**

АПАРАТНА РЕАЛІЗАЦІЯ ПРИСТРОЮ ШИФРУВАННЯ МОВНОЇ ІНФОРМАЦІЇ

В даній роботі запропонована апаратна реалізація пристрою шифрування мовної інформації хаотичними послідовностями, що генеруються на основі одномірних дискретних хаотичних відображень. Роботу пристрою досліджено на прикладі шифрування гармонійного сигналу. Проведені дослідження пристрою підтвердили можливість застосування мікроконтролерів для шифрування мовної інформації з використанням сучасних криптостійких алгоритмів.

Ключові слова: мовна інформація, мікроконтролер, псевдовипадкова послідовність, крипостійкість.

Вступ

Сучасні телекомунікаційні системи вимагають забезпечення високої прихованості і конфіденційності інформації, що передається по каналах зв'язку. Забезпечення конфіденційності інформації сучасних телекомунікаційних систем можливе шляхом її шифрування інформації за допомогою хаотичних послідовностей.

Найефективнішим способом захисту мовної інформації від загроз (отримання несанкціонованого доступу , втрати цілісності та автентичності інформації) є її криптографічне перетворення. На даний час для захисту мовної інформації використовуються: цифрове скремблювання, потокове шифрування (гамування), стандартне шифрування. Ці методи володіють певними недоліками, зокрема : скремблювання може викликати додаткові затримки при передаванні аудіо інформації, що викликано самим алгоритмом скремблювання ; стандартне криптографічне шифрування по одному з відомих алгоритмів забезпечує задовільний захист, але є витратним з точки зору швидкості і складності обчислень [1].

Основна частина

Найкращим (з точки зору швидкості та складності обчислень) способом захисту аудіоінформації є побітове додавання по модулю 2 (операція XOR) оцифрованих відліків вхідної послідовності мовної інформації (повідомлення) з певною послідовністю (ключем шифрування), що може бути сформована наприклад генератором хаотичних послідовностей. В якості послідовності гамування можуть використовуватися псевдохаотичні послідовності , алгоритми генерування яких реалізовані на базі явища динамічного хаосу , що є чутливим до зміни початкових умов.

Практичну реалізацію пристроїв шифрування мовної інформації можна здійснити з використанням сучасної елементної бази (мікроконтролерів, програмованих логічних інтегральних схем та ін.), що забезпечує покращення їх масогабаритних показників, розширення функціональних можливостей та підвищення швидкості передавання даних[2,3]

В даній роботі запропонована апаратно-програмна реалізація пристрою шифрування аудіоінформації хаотичними послідовностями, що генеруються на основі одномірних дискретних хаотичних відображень. Структурна та електрична схема якого приведена на рис.1 та рис.2, відповідно.

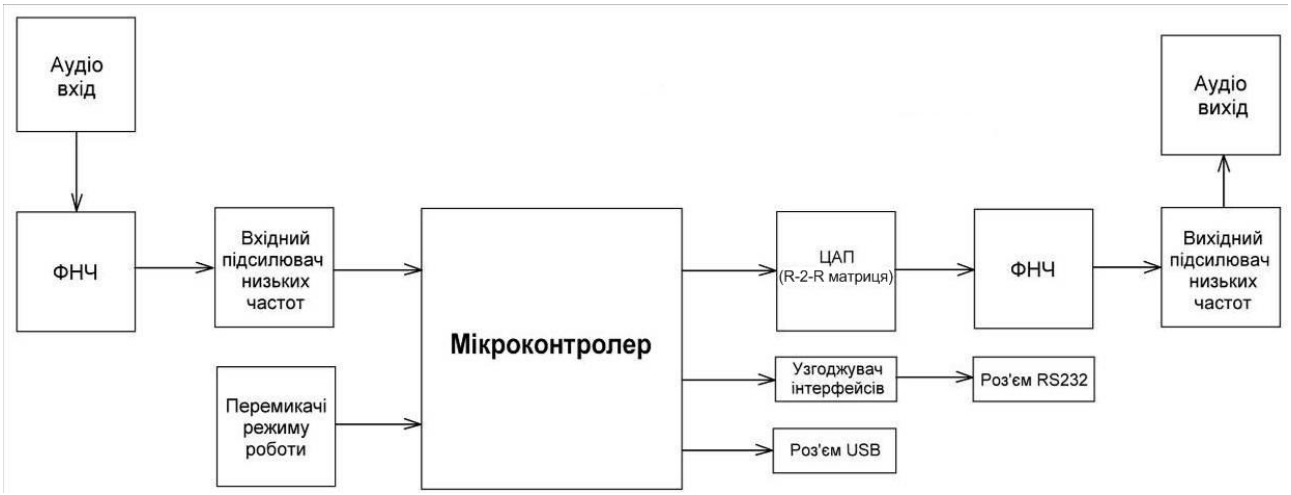

Рис.1. Структурна схема пристрою шифрування мовної інформації

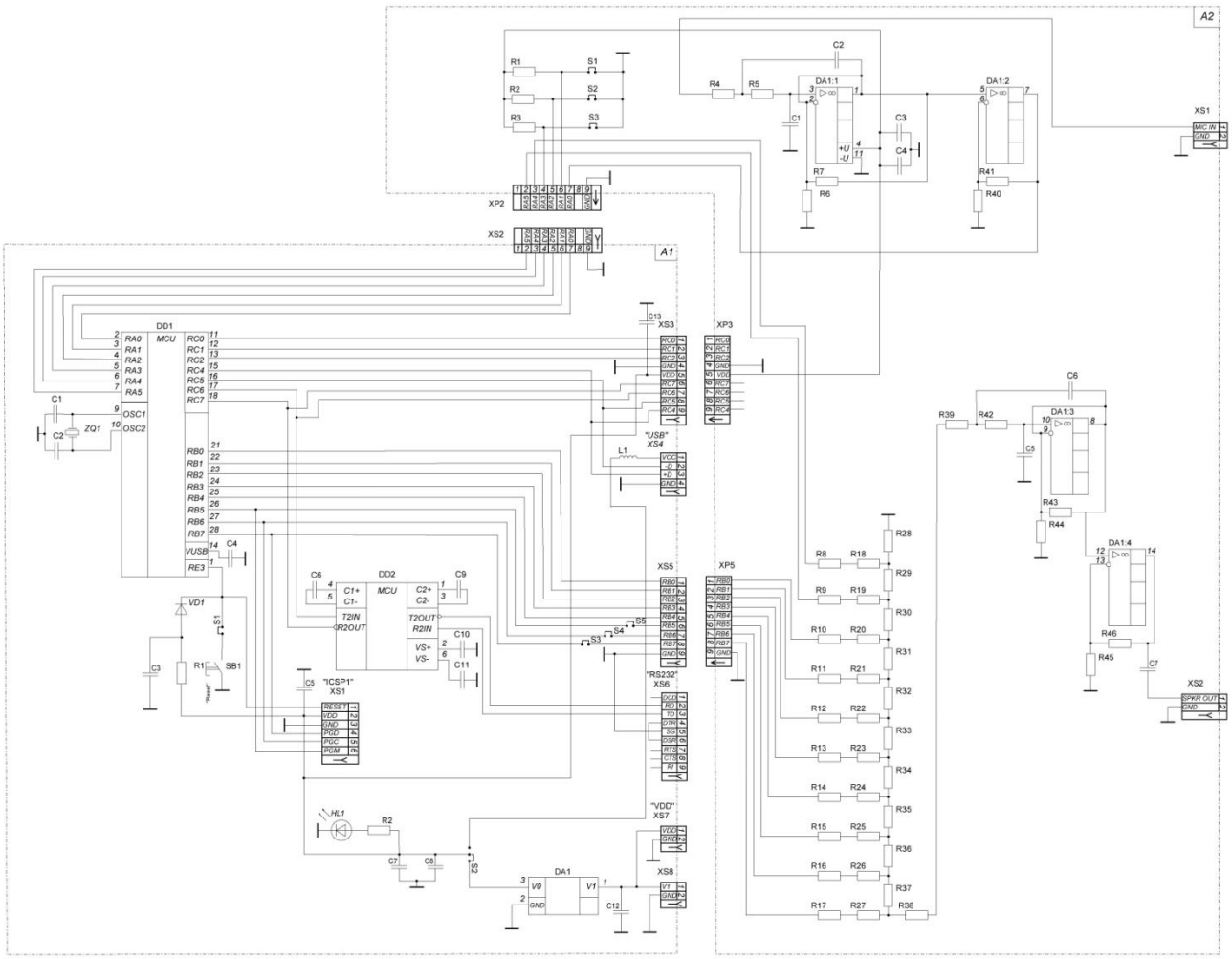

Рис.2. Схема електрична принципова пристрою шифрування мовної інформації

Даний пристрій складається з модуля керування А1 (основного) та виконавчого модуля А2.

Оброблення мовної інформації здійснюється за допомогою мікроконтролера PIC 18F2550 з вбудованим 10-бітним АЦП. Даний пристрій може працювати в режимах:

генерування хаотичного сигналу (генератор шуму), шифрування (дешифрування), повторювача. Необхідний режим роботи пристрою встановлюється перемичками S1-S3.

Алгоритм шифрування

Відфільтрований сигнал з мікрофону підсилюється та подається подається на вхід АЦП мікроконтролера, що здійснює його оцифровування з частотою дискретизації 8 КГц.

Для генерування цифрових хаотичних послідовностей використовується одномірне дискретне відображення, що носить назву логістичного рівняння [4,5] :

$$x_{n+1} = \lambda \cdot x_n (1 - x_n), \quad (1)$$

де λ – параметр, x_0 - початкова умова для генерування послідовностей. Генерування хаотичної послідовності у відповідності з цим рівнянням має місце при значеннях параметру $\lambda \in [3{,}65 \div 3{,}95]$. В нашому випадку генерування послідовностей здійснювалось при значенні параметру λ рівному 3,85 та початковій умові x_0 =0,5. Оцифрована мовна інформація m_i, додається за модулем 2 з елементами хаотичної послідовності z_i, утворюючи зашифровану послідовність s_i:

$$s_i = m_i \oplus z_i . \quad (2)$$

При створенні систем передавання інформації з використанням даних пристроїв на передавальній та приймальній сторонах обмін зашифрованою інформацією а також зв'язок контролера з комп'ютером може здійснюватися через порти USART (роз'єм XP2) і USB (роз'єм XP1). Мікросхема MAX232 (DD2) здійснює узгодження інтерфейсу RS-232 (COM-порту комп'ютера) з портом USART мікроконтролера. При цьому пристрій також може працювати і в режимі дешифрування (на приймальній стороні).

Дешифрування інформації здійснюється шляхом додавання за модулем 2 отриманої зашифрованої інформації з елементами хаотичної послідовності, що генерованої на приймальній стороні з використанням того ж логістичного рівняння при тих же початкових умовах [6-8]. Після дешифрування корисна мовна інформація передається на зовнішній ЦАП, що складається з R-2-R матриці та ключів вихідного порта мікроконтролера. Після перетворення, аналоговий сигнал через ФНЧ та вихідний підсилювач низьких частот передається на аудіо-вихід.

Криптостійкість пристрою обумовлена простором ключів для генерування послідовностей, що є значенням параметра логістичного відображення λ та початкового значення x_0. Обсяг простору ключів буде визначатися за формулою [9] :

$$N = (10^n)^2 , \quad (3)$$

де n – точність введенння параметрів (кількість знаків після коми).

Значення початкової умови x_0 та параметру λ задаються при програмуванні мікроконтролера. Генерування послідовностей та процес шифрування здійснюється на програмному рівні. Програма для мікроконтролера написана на мові програмування програмування С згідно алгоритму, приведеного на рис.3.

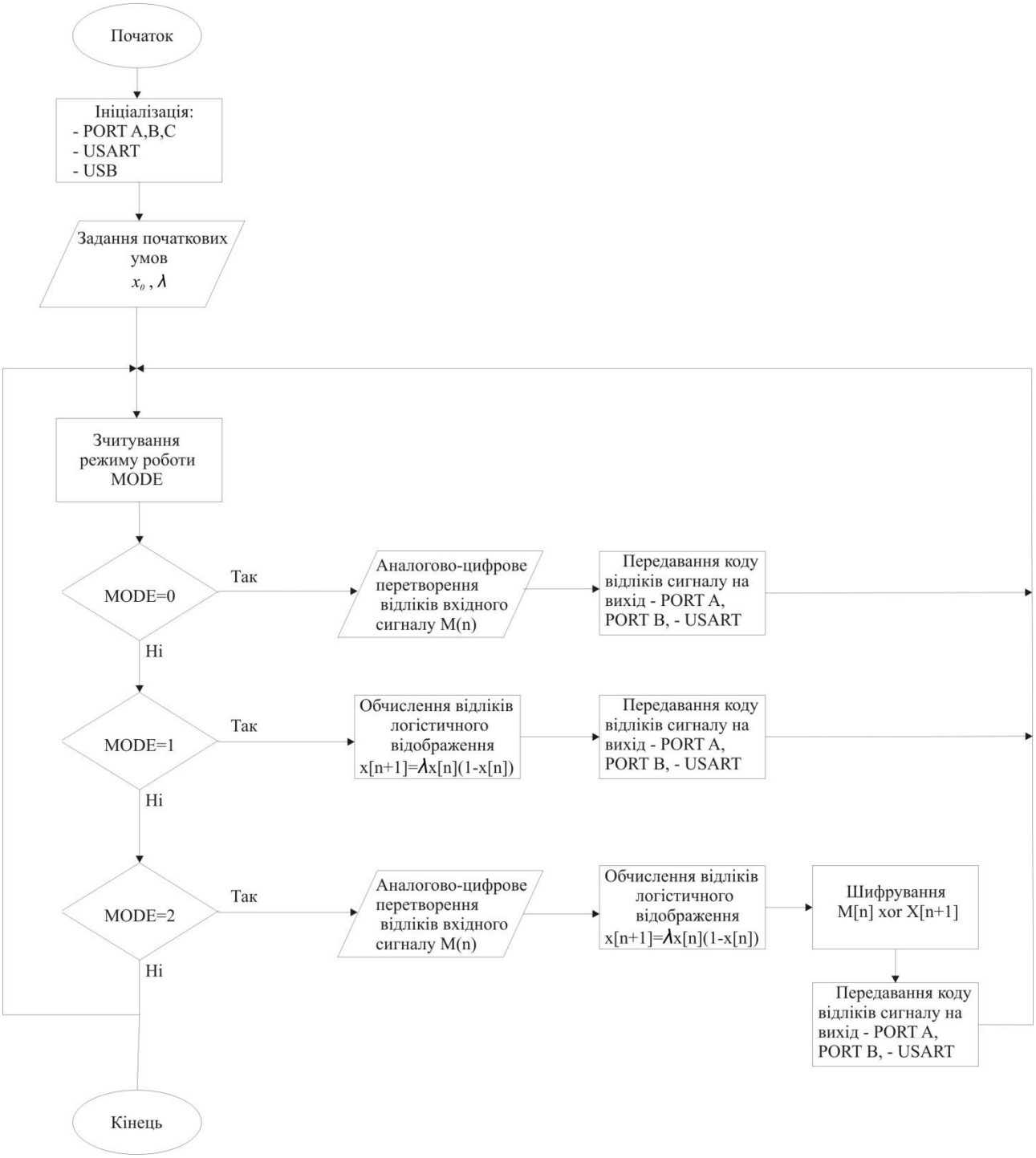

Рис.3. Алгоритм роботи програми керування мікроконтролера

Результати роботи

Для експериментального дослідження процесу шифрування інформації було використано гармонійний сигнал амплітудою 2В та частотою більше 100Гц. Результати досліджень приведені на рис. 4-9.

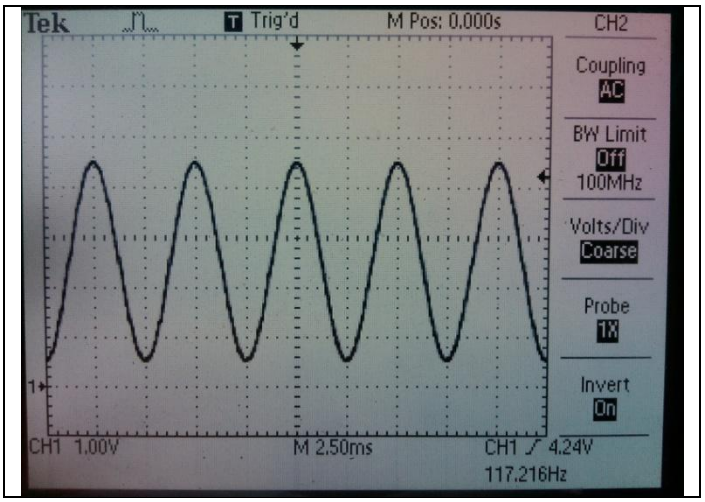

Рис.4. Сигнал на виході пристрою в режимі повторювача

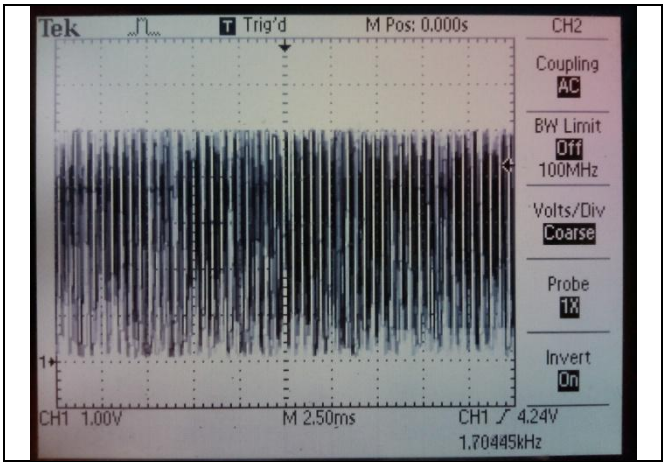

Рис.5. Вихідний сигнал в режимі генерування хаосу

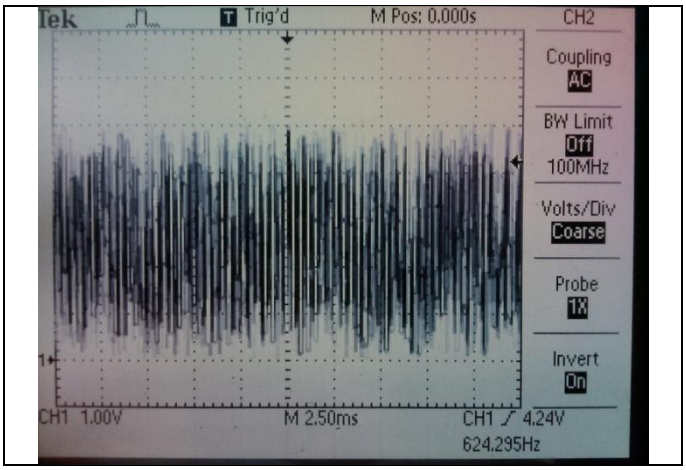

Рис.6. Зашифрований сигнал (сигнал + шум)

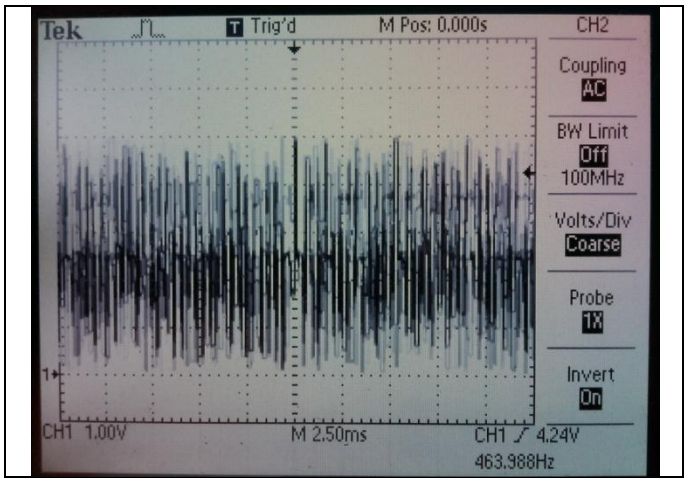

Рис.7. Вихідний сигнал (шум) при заземленому вході

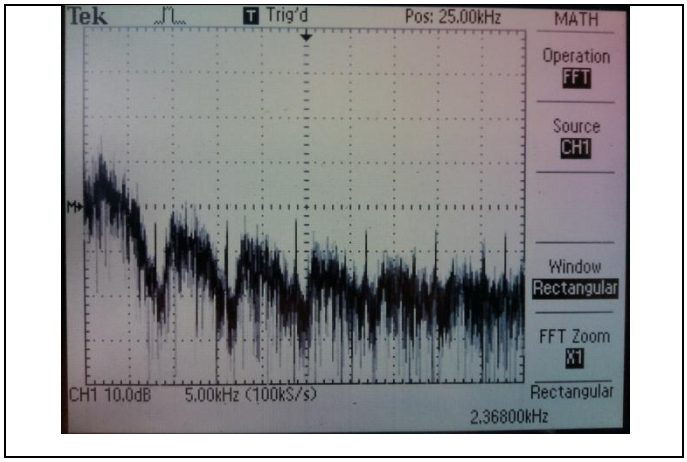

Рис.8. Спектральне представлення хаотичного сигналу

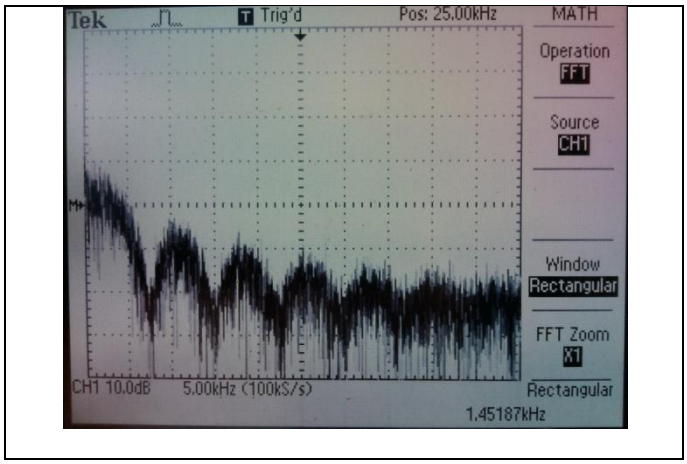

Рис.9. Спектральне представлення зашифрованого сигналу

Висновки

В даній роботі запропонована апаратна реалізація пристрою шифрування мовної інформації. Шифрування здійснюється хаотичними послідовностями, що генеруються на основі одномірних дискретних хаотичних відображень.

Проведені дослідження пристрою підтвердили можливість застосування мікроконтролерів для шифрування мовної інформації із застосуванням сучасних криптостійких алгоритмів. Системи зв'язку на основі таких пристроїв є криптостійкими, що обумовлено наявністю великої кількості ключів шифрування.

Література

1.Шахов В.Г., Нопин С.В. Моделирование защиты речевой информации с помощью персонального компьютера // Омский научный вестник, 2004, № 4(29). – С .124–126.

2.Стасєв Ю.В., Васюта К С., Женжера С.В. Інформаційні системи на основі динамічного хаосу // Системи озброєння і військова техніка. №1(17). – 2009. – С. 134-138.

3.Y. Mao, W. Liu, Z. Li, P. Li, A. Halang, "A Chip Performing Chaotic Stream Encryption", *Studies in Computational Intelligence (SCI), 42, 307-332 (2007)*

4.Савельев С.В. Счетное множество бинарных последовательностей для широкополосных систем связи на основе системы с динамическим хаосом / 111 Всероссийская конференция «Радиолокация и радиосвязь» – ИРЭ РАН – 2009, 26-29 октября, – С.488 – 493

5.Політанський Р.Л., Шпатар П.М., Гресь О.В., Ляшкевич В.Я. Шифрування інформації з використанням псевдовипадкових гаусових послідовностей // Восточно-европейский журнал передовых технологий. – 2012. – №6/11(60). – С. 8–10.

6.Політанський Р.Л., Політанський Л.Ф., Гресь О.В., Галюк С.Д. Система передавання даних з використанням генераторів хаосу // Всеукраинский межведомственный научно-технический сборник «Радиотехника». – 2011. – № 164. – С. 66-71.

*7.*Abd al-Karim, Maysa, Abd al-Jalil, Iman Qays, "Speech Encryption Using Chaotic Map and Blowfish Algorithms", *Journal of Basrah Researches (Sciences) Vol.(39), No.(2), 68-76 (2013)*

*8.*C. Cruz-Hernández, E. Inzunza-González, R. López-Gutiérrez, H. Serrano-Guerrero, E. García-Guerrero, "Encrypted audio communication based on synchronized unified chaotic systems", *World Academy of Science, Engineering & Technology. 42, 475 (2010)*

9.Политанский Р.Л., П.М. Шпатарь, А.В. Гресь, А.Д. Верига Система передачи данных с шифрованием хаотическими последовательностями // Технология и конструирование в электронной аппаратуре. – 2014. – №2-3. – С. 28-32.

Надійшла 06.07.2014 р. Рецензент: д.т.н., проф. Шелест М.Є.