III Висновки

1. Використання у алгоритмі шифрування AES вузлів заміни на основі арифметичних операцій в скінчених полях забезпечує суттєве спрощення програмно-апаратної реалізації. Існує практична можливість розробки криптопроцесору на базі дешевих мікроконтролерів з відносно малими вимогами до програмних ресурсів. При цьому гарантована швидкість обробки інформації становить 64 кбіт/с.

2. Наявність безкоштовно розповсюджуваного налагоджувального програмного забезпечення (ПЗ) фірми *Microchip* типу MPLAB дозволяє організувати його використання в учбовому процесі для підготовки студентів за фахом „Інформаційні технології та захист інформації" для практичного вивчення особливостей функціонування та побудови алгоритму AES на основі мікроконтролерів. Важливо підкреслити, що забезпечується легальне використання ПЗ з оглядом на Розпорядження КМ України № 247 – р від 15 травня 2002 р. „Про затвердження Концепції легалізації програмного забезпечення та боротьби з нелегальним його використанням". З іншого боку, налагоджувальне ПЗ розробки надвеликих інтегральних схем (НВІС) фірм ALTERA, XILINX має вартість від сотень до тисяч доларів, тобто практично недоступне для використання у вищих навчальних закладах. Недоступною (з фінансових міркувань) є також закупівля готових проектів НВІС (core – технологія).

3. Відносна простота програмно-апаратної реалізації алгоритму AES може привести до зростання продажу засобів КЗІ на його основі, що відповідно загострить проблему використання сертифікованих засобів захисту від несанкціонованого доступу до інформації.

Література: ***1.*** *Вакка Дж. Секреты безопасности в Internet: Пер. с англ. // К.: Діалектика Киев, 1997. - 505 с.* ***2.*** *Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. // М.: Радио и связь, 1987. -391 с.* ***3.*** *R. Lidl and H. Niederreiter, Introduction to finite fields and their application, Cambridge University Press, 1986.* ***4.*** *Microchip: Implementation of the Data Encription Standard Using PIC17C42. http://www.microchip.com.* ***5****. Microchip: Application Note AN821 Advanced Standard Using the PIC16XXX. http://www.microchip.com.*

УДК 681.3.34.

ГЕНЕРАТОР ТЕСТОВОЇ ПОСЛІДОВНОСТІ ІКМ 30 (Е1) ІНТЕРФЕЙСУ

Всеволод Семенюк, Володимир Кишкан, Геннадій Леоненко*

ДСТСЗІ СБ України

** СФ СБ України ВІТІ НТУУ "КПІ"*

Анотація: **Розглянуто генератор тестової послідовності для забезпечення досліджень ПЕМВН цифрового комутаційного обладнання, що має інтерфейс ІКМ-30 (Е1) згідно з рекомендаціями CCIT G.704 для ІКМ 30.**

Summary: **In the article designing test generator for CEPT trunk digital link interface conforming to CCIT Recommendation G.704 for PCM 30.**

Ключові слова: **Тестове обладнання, ІКМ 30.**

I Вступ

Проведення досліджень побічних електромагнітних випромінювань та наведень (ПЕВМН) певною мірою залежить від пошуку інформативних складових сигналу у цифровій телекомунікаційній техніці, що перевіряється. Для спрощення цього завдання формують відповідні тестові сигнали (ТС), що відповідають наступним вимогам: ідентичність робочому сигналу; максимальне спектральне навантаження; помітність на фоні завад.

Як генератор ТС можна використовувати, по-перше, стандартну апаратуру. Але вона часто є багатофункціональною, має значні габаритні розміри, складається із багатьох блоків, що не дозволяє використовувати її як мобільний комплекс і викликає певні труднощі при проведенні дослідження ПЕВМН. По-друге, можна використати обладнання, яке саме проходить дослідження завдяки введенням у тестовий режим, завантаживши відповідне програмне забезпечення (якщо це передбачено). По-третє, можна розробити спеціальне додаткове оснащення порівняно малої вартості, яке б виконувало необхідні функції у мобільному варіанті.

Останній шлях розглянемо більш детально.

II Загальні відомості інтерфейсу ІКМ 30 (Е1)

Інтерфейс забезпечує обмін інформацією та тактовими сигналами на швидкості 2048 кбіт/с [1].

Номінальна форма імпульсів сигналів стику – прямокутна.

Вимірювальний опір навантаження – 120 ± 1 Ом.

Номінальна напруга імпульсів сигналу будь-якої полярності – 3В.

Пікова напруга будь-якої полярності при відсутності імпульсів стикового сигналу, не більше – 0,3 В.

Вихідний опір – (120 ± 24) Ом.

Номінальна довжина імпульсу – 244 нс.

Структура циклу групового сигналу стику:

- номінальна довжина циклу – 125 мкс;
- кількість тактових інтервалів у циклі – 256;
- кількість послідовних канальних інтервалів (КІ) у циклі – 32;
- нумерація КІ від 0 до 31 (КІ0 – КІ31), з них службових – 2(1), інформаційних – 30(31);
- кількість символів (розрядів) у канальному інтервалі – 8. Нумерація від 1 до 8;
- номінальна довжина надциклу – 2 мс.

Структура канального інтервалу 0 (КІ0).

Структура КІ0 наведена в табл. 1.

М – біт зарезервовано для міжнародного використання (при невикористанні встановити на „1”).

А – біт індикації аварії („1” – аварія, „0” – нормально).

Р, С, В, Т, У – біти, зарезервовані для національного використання.

Р, У – біти сигналів автоматичної системи оперативно-технічного управління.

С – біт синхронізації мережі або аналогічно Р, У.

Т, В – біти для використання за спеціальним призначенням.

Біти Р, С, В, Т, У при невикористанні – встановити на „1”.

Структура канального інтервалу 16 (КІ16).

Структура КІ16 наведена в табл. 2.

Для забезпечення передачі сигналів управління та взаємодії АТС обмін інформації здійснюється надциклами, кожний з яких складається із 16 циклів. Цикли нумеруються від 0 до 15. Сигнал надциклового синхронізму має вигляд „0000”. Він передається у КІ16 циклу 0. У КІ16 у циклах 1 – 15 передається інформація сигналізації двох мовних каналів.

Таблиця 1 – Структура канального інтервалу 0

КІ0	Розряди КІ							
	1	2	3	4	5	6	7	8
Парний (має цикловий синхросигнал)	М	0	0	1	1	0	1	1
Непарний (без циклового синхросигналу)	М	1	А	Р	С	В	Т	У

Таблиця 2 – Структура канального інтервалу 16

КІ16 цикл 0		КІ16 цикл 1		КІ16 цикл 15	
0000	ХУХХ	АБВГ біти для телефонного каналу 1	АБВГ біти для телефонного каналу 16	АБВГ біти для телефонного каналу 15	АБВГ біти для телефонного каналу 30

Х – біт, встановлено на „1”.

У – біт індикації втрати надциклової синхронізації. При відсутності аварії встановлено на „0”.

У кожному з циклів 1–15 КІ16 передається сигнальна інформація двох телефонних каналів 1 та 16, 2 та 17, 3 та 18 і далі до 15 та 30. Якщо біти Б, В, Г не використано, то А=0, Б=1, В=0, Г=1.

III Функціональна схема генератора тестової послідовності (ГТП)

ГТП розраховано на роботу по інтерфейсу ИКМ 30 з швидкостю групового потоку 2048 кбіт/с. Тип лінійного коду, структура сигналу (згідно з рекомендаціями G.703, G.704) – AMI або HDB3.

Заповнення інформаційних канальних інтервалів (КІ1 – КІ5, КІ17 – КІ31) має вид 101010..., або спеціально розрахована послідовність для забезпечення максимальної енергетики спектру випромінювання.

Для забезпечення виявлення спектральних складових сигналу введено послідовність заповнення інформаційних канальних інтервалів.

Управління інформаційними та контрольними складовими потоку 2048 кбіт/с E1 побудовано на мікросхемі MT9079 (розширений контролер E1). Спеціалізована мікросхема реалізує рекомендації CCITT G.704, G.706, G.732, G.775, G.796, I.431 та ETSI ETS 300 011 та дозволяє встановлення лінійних кодів RZ, NRZ (оптичний інтерфейс) та біполярного NRZ.

Гальванічну розв'язку та узгодження з опором лінії забезпечує мікросхема MH89793 (лінійний інтерфейс E1) [2].

Генерація необхідних керуючих та інформаційних сигналів виконана на базі 8-розрядних мікроконтролерів.

Додатково передбачено можливість проведення верифікації послідовності, що приймається, відносно тієї, що передається. ГТП можливо застосовувати як допоміжне обладнання при проведенні верифікації засобів КЗІ, призначених для роботи з каналом E1. При цьому функція заповнення інформаційних канальних інтервалів відключається. Зміна функціональних можливостей досягається шляхом перепрограмування мікроконтролерів, що виробляють керуючі та інформаційні сигнали, або введенням відповідного перемикача "Режим" – для забезпечення завантаження необхідної частини асемблерної програми мікроконтролера. Результат верифікації відображено на індикаторі кількістю помилок за один запуск тестової програми.

Функціональну схема ГТП наведено на рис 1.

Приймач-передавач (LIU Line Interface Unit) виконує наступні функції:

- перетворює сигнал на передачу від контролера E1 у псевдо-потрійну форму;
- перетворює сигнал при прийманні з лінії із псевдо-потрійної форми у бінарну на вході контролера E1;
- виділяє з потоку даних при прийманні частоту синхронізації 2.048 МГц.

Контролер E1 призначено для виконання наступних функцій:

- формування сигналу при передаванні у форматі E1 на основі вхідного потоку даних та сигналів керування;
- виділення із потоку E1 при прийманні окремо потоку даних та сигналів керування.

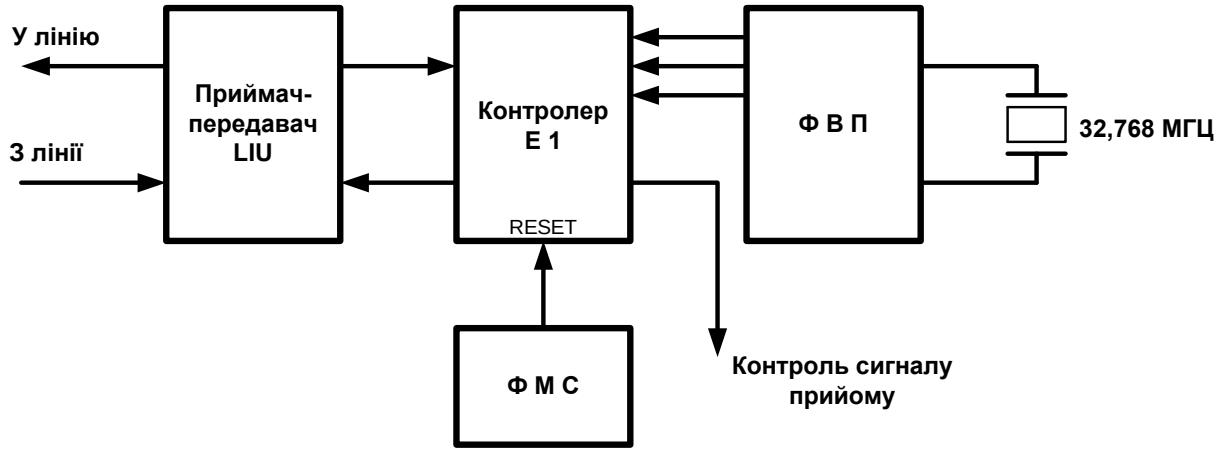

Рисунок 1 – Функціональна схема ГТП

Формувач вихідного потоку (ФВП) генерує інформаційний та керуючі потоки за формою, необхідною для роботи контролера E1.

Формувач сигналу заповнення (ФСЗ) виробляє сигнали керування ФВП та контролера E1, або вирішує завдання верифікації.

IV Опис роботи ГТП

Контролер E1 має три режими управляючого інтерфейсу:

- паралельний мікроконтролерний порт;
- послідовний мікроконтролерний порт;
- спеціальний режим так званої ST-BUS.

У даному випадку використано останній режим як такий, що має просту програмно-апаратну реалізацію, але перші два дозволяють у більш повному обсязі використовувати функціональні можливості контролера Е1 типу МТ9079.

Для контролю та передавання інформації призначено наступні контакти:

- контакт 21 CSTi0 – вхід канальних інтервалів ST – BUS для передавання сукупності керуючих сигналів (Master Control Words page 1); інформаційне наповнення цього входу повністю відповідає початковим установкам згідно з технічним описом на мікросхему МТ9079, крім бітів, що відповідають за кодування вихідного сигналу (встановлено 10 - NRZ код, потрібно 00 - RZ код);
- контакт 23 CSTi1 – вхід канальних інтервалів ST – BUS для безпосереднього керування кожним з інформаційних канальних інтервалів потоку Е1 (Master Status Words page 2); для роботи ГТП цей вхід не використовується (постійно передається логічний “0”);
- контакт 35 CSTi2 – вхід передавання сигнальної інформації телефонних каналів (див. біти АБВГ, табл. 2);
- контакт 30 DSTi – вхід канальних інтервалів для даних;
- контакт 24 C2i – вхід тактової частоти 2,048 МГц;
- контакт 25 F0i – вхід кадрового синхроімпульсу.

Всі сигнали, що поступають на вищевказані контакти контролера Е1, мають бути синхронними відносно тактової частоти 2,048 МГц та кадрового синхроімпульсу [3].

В табл. 3 надано заповнення канальних інтервалів на всіх входах. При такому заповненні забезпечується реалізація вимог протоколу Е1 щодо табл. 1 та табл. 2.

Біти 7 – 4 входу CSTi2 відповідають бітам АБВГ сигнальної інформації телефонних каналів у всіх КІ, окрім КІ0 та КІ16.

Контролер Е1 виконує функцію перетворення сигналів на входах DSTi, CSTi0, CSTi1 та CSTi2 у інформаційний потік Е1.

Усі сигнали керування мікроконтролер ФВП формує від опорного кварцового генератора 32.768 МГц.

Таблиця 3. Заповнення інформаційних та керуючих сигналів

Канальний інтервал	DSTi								CSTi0								CSTi2							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
2	0	1	0	1	0	1	0	1	1	0	0	1	1	1	1	1	1	0	1	0	0	0	0	0
3	0	1	0	1	0	1	0	1	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	0
4	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
5	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
6	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
7	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
8	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
9	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
10	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
11	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
12	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
13	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
14	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
15	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
16	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
17 – 31	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0

Конструктивно ГТП виконано у вигляді екранованого модуля з відповідними роз’ємами для підключення до каналу типу Е1 та джерела живлення. На фронтальній стороні модуля розташовані органи керування та індикації. Завдяки незначному струму електричного живлення (меншому 50 mA), є можливим використання батарейного живлення при проведенні дослідження ПЕМВН.

V Висновки

На даному етапі при недостатньому забезпеченні відповідною тестовою та контрольно-перевірочною апаратурою у галузях ТЗІ та КЗІ доцільно рекомендувати використання розробленого генератора для проведення необхідних випробувань. Спеціалізована елементна база для телекомунікаційних технологій у поєднанні із 8-розрядними мікроконтролерами дає змогу розробляти апаратуру з високими технічними характеристиками для проведення досліджень щодо ПЕМВН цифрової телекомунікаційної техніки. Простота зміни наповнення інформаційних та службових канальних інтервалів потоку даних 2,048 МГц формату E1 завдяки використанню мікроконтролерів дозволяє генерувати тестові послідовності будь-якої інформаційної функції. Окрім того вищезазначений ГТП можливо використовувати для ремонту та перевірки відповідного стандартного телекомунікаційного обладнання. Надалі планується поєднати ГТП за допомогою ISA-шини з ПЕОМ, що дозволить візуально аналізувати потік E1 та проводити обробку накопиченої інформації.

Література: ***1.*** *MITEL. Application Note MSAN-128. Implementing an ISDN Architecture. Using ST-BUS.* ***2.*** *MITEL. MH89793. E1 Line Interface Unit (LIU) with Selectable Impedance. Preliminary Information.* ***3.*** *MITEL. MT9079. Advanced Controller for E1.*