Системы управления обучением/Системы управления учебным контентом (LMS/LCMS) решения и сервисы. Том 2. 2009год»

**References**

1. Advanced Distributed Learning. Sharable Content Object Reference Model (SCORM) 2004.
2. http://www.distance-learning.ru/db/el/6BA99B5047DB50F3C3256C2400258647/doc.html
3. http://elearning-ua.blogspot.com/2008_10_01_archive.html
4. V. V. Dyadichev, V.Yu.Vashchenko Analysis of means of the organization of e-learning//Vesnik LNU of a name of Taras Shevchenk No. 12 (223), Ch. I, 2011, page 97-107.
5. Report materials "The program of researches of the market of technologies of remote learning in the CIS. Training/management system management systems educational content (LMS/LCMS) of the decision and services. Volume 2. 2009"

Рецензія/Peer review : 8.9.2013 р. Надрукована/Printed :23.11.2013 р.
Рецензент: Параска Г.Б., д.т.н., проф.

УДК 621.396.662

О.І. ПОЛІКАРОВСЬКИХ
Хмельницький національний університет

# ПРИНЦИПИ ПОБУДОВИ СУМАТОРІВ ГАЛУА ТА ЇХ ЗАСТОСУВАННЯ У СУЧАСНИХ СИСТЕМАХ СИНТЕЗУ СИГНАЛІВ

*Розглянуто принципи побудови суматорів Галуа та їх місце у сучасних системах синтезу радіосигналів. Запропоновані структури синтезаторів із фазовими акумуляторами на основі суматорів Галуа, що дасть можливість збільшити розрядність синтезаторів, покращити їх частотні характеристики у сторону розширення діапазону синтезованих сигналів. Розглянуто принципи апаратної реалізації суматорів у полях Галуа.*

Ключові слова: **:** обчислювальний синтезатор частоти, фазовий акумулятор, суматор, поле Галуа

O.I. POLIKAROVSKYKH
Khmelnitsky National University, Khmelnitsky, Ukraine

# GALOIS ADDERS IN MODERN DIRECT DIGITAL SYNTHESIZERS

*Principles of construction of Galois adders and their place in modern systems synthesis of radio signals. The proposed structure of the phase synthesizer based on Galois field adders, which will increase the bit synths and improve their frequency response range expansion into the side of the synthesized signals. The principles of the hardware implementation of adders in Galois fields was proposed.*

Keywords: Galois field, adder, *direct frequency synthesizer (DDS)*.

**Постановка задачі**

Особливістю синтезаторів прямого синтезу є те, що частота, амплітуда та фаза сигналу, що сформовані на їх виході, відомі для будь якого моменту часу і можуть бути запрограмовані. Параметри таких синтезаторів практично не залежать від температури і старіння елементів. Єдиним елементом який, має притаманну аналоговим системам нестабільність є цифро-аналоговий перетворювач (ЦАП). Завдяки відмінним технічним характеристиками і високій швидкості переналаштування частоти та фази прямі цифрові синтезатори (DDS) набувають все ширшого застосування. Основними перевагами синтезаторів є: високе розрізнення по частоті і фазі, швидке пере налаштування частоти (фази), пере налаштування за частотою без розриву фази синтезованого сигналу і без викидів напруг на виході, можливість програмним методом впливати на модуляційні характеристики сигналів синтезаторів [1].

Розрізнення за частотою досягає тисячних частин герца для вихідної частоти до декількох десятків мегагерц, що є недосяжним параметром для інших систем синтезу. Сучасні синтезатори DDS виготовляється за субмікронною КМОП - технологією з використанням логіки з напругою живлення у 3 вольта і мініатюрних корпусів. Однак використання дискретизації та цифро-аналогового перетворення, яке використовуються накладають певні обмеження:

1) максимальна вихідна частота не може бути вище половини тактової (на практиці вона ледь досягає $1/3\,f_{такт}$), проте завдяки застосуванню нових технологій тактова частота постійно зростає (Синтезатор AD9914 при тактові частоті 3,5 ГГц здатен синтезувати гармонійний сигнал частотою 1,4 ГГц з прийнятними рівнями гармонійних складових);

2) окремі бічні складові у спектрі сигналу на виході синтезатора DDS можуть бути значно більшими, ніж у синтезаторах, що побудовані на основі системи ФАПЧ, бо спектральна чистота вихідного сигналу синтезатора DDS залежить від характеристик ЦАП;

3) потужність, що споживається синтезатором практично прямо пропорційна тактовій частоті синтезатора і може досягати одиниць ват для високочастотних синтезаторів, тому на високих частотах DDS можуть виявитись неприйнятними для пристроїв з живленням від батарей;

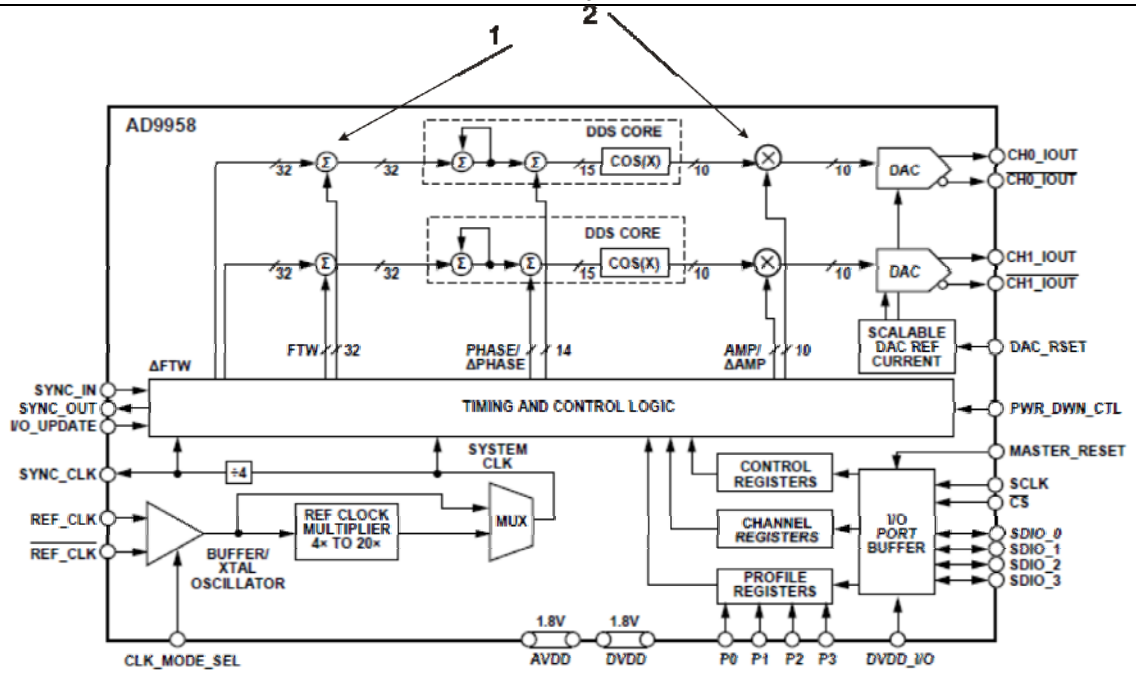


**Рис.1 Функціональна схема синтезатора AD9958**
**(1 - 32-х бітний суматор, 2 - 10-ти бітний перемножувач)**

В системах цифрового синтезу особливе місце займає суматор [3] у якості фазового акумулятора та як частина різноманітних блоків модуляції вихідного сигналу. На рис. 1 представлено функціональну схему сучасного синтезатора прямого цифрового синтезу AD9958, з якої добре видно важливість оптимального схемотехнічного рішення багаторозрядного (у нашому випадку 32-х бітного) суматора і перемножувачів (основою яких є суматори). Отже, саме від будови суматора залежать тактико-технічні параметри синтезаторів прямого цифрового синтезу [3]. Від ефективності реалізації накопичувального суматора залежать апаратні та часові характеристики прямого цифрового синтезатора (DDS) частот і сигналів. Таким чином, завдання мінімізації часу обчислення і зменшення апаратних витрат зводиться до оптимізації операцій підсумовування, яка використовується як у ядрі синтезатора так і у різноманітних допоміжних блоках, що необхідні для формування повноцінного вимірювального або телекомунікаційного сигналу. Одним з розв'язків поставленої задачі може бути реалізація синтезаторів в кінцевих полях (полях Галуа).

Аналіз досліджень та публікацій

Задачу підвищення швидкості та надійності обчислень можна розглядати з двох сторін. З одного боку це апаратний рівень, фундаментальними обмеженнями на якому є технічні можливості створення елементної бази – зменшення розмірів кристалів, збільшення частоти синхронізації( тактової частоти ) , рішення проблем тепловідведення та ін. Багато в чому цей рівень визначається сучасним станом фундаментальних наук, перш за все, фізики. З іншого боку це - математико - алгоритмічний рівень обчислень, і фундаментальними обмежуючими факторами тут виступають , в числі інших , необхідність послідовного обчислення, коли наступний етап (крок) частково або повністю залежить від попередніх кроків. Навіть найпростіші арифметичні операції додавання і множення при реалізації їх обчислювачами з архітектурою фон – Неймана здійснюються побітно, і обчислення кожного наступного біта залежить від результату операції над попередніми бітами (у даному випадку це знак переносу - carry sign ), існують і інші обчислювальні архітектури, в яких акцент зроблено на паралельність і масовість обчислень. Велику популярність зараз мають нейронні мережі, які, володіючи алгоритмічної універсальністю машини Тьюринга [4], вже довели своє перевагу в слабо формалізованих завданнях, пов'язаних з необхідністю навчання. Використання системи залишкових класів (СЗК) і медулярних обчислень дозволяє істотно збільшити швидкість арифметичних обчислень за рахунок паралельного виконання операцій над залишками[5]. Сучасна апаратна база дозволяє також замінювати арифметичні операції над залишками однотактним і табличними вибірками. Довгий час модулярна арифметика розглядалася як цікаве, але суто теоретичне питання через складність виробництва обчислювальних структур для її реалізації. Сучасний розвиток технології інтегральних схем зробило можливим використання модулярної арифметики у багатьох областях цифрової обробки сигналів , розпізнавання образів і інших завдань , що вимагають інтенсивних обчислень . Базовим поняттям медулярної арифметики є «поле».

Полем називають множину з двома операціями – додаванням та множенням, які відповідають наступним аксіомам[5]:

1) Множина формує комутативну групу по додаванню.

2) Поле замкнене відносно множення і множина ненульових елементів формує комутативну групу за множенням

3) Дистрибутивний закон виконується для будь-яких елементів поля.

Широко відомими є приклади полів з нескінченним числом елементів: множина дійсних чисел, множина комплексних чисел, множина раціональних чисел. Існують також поля із скінченною кількістю елементів. Поле з

$q$ елементами, якщо воно існує, називається скінченним полем, або полем Галуа (Galois Fields -GF) на честь французького математика Евариста Галуа, і позначається GF(q).

Скінченні поля можна описати за допомогою таблиць додавання та множення. Віднімання та ділення однозначно визначається таблицями додавання та множення. Наведемо приклад поля GF(5)={0,1,2,3,4}, яке повністю описується таблицями 1.1. та 1.2:

Для довільного поля, як нескінченного так і скінченного, можна застосовувати майже усі відомі алгоритми обчислення. Це відбувається тому, що більшість процедур, що використовуються у полях дійсних та комплексних чисел, залежить лише від формальної структури поля приклад якої наданий вище і не залежить від характеристик конкретного поля.

Таблиця 1.1

Додавання елементів поля GF(5)

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

Таблиця 1.2

Множення елементів поля GF(5)

| * | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Розглянемо більш докладно систему залишкових класів, яка дає можливість обчислювати значення елементів полів у непозиційній системі числення. Проаналізуємо можливість застосування математичного теоретико-числового базису прямих ортогональних сум полів Галуа. Даний базис визначається властивостями Китайської теореми про залишки і описується системою дискретних ортогональних функції Віленкіна – Крестенсона у системі взаємно простих модулів $P_1, P_2 \ldots P_k$. Цей базис породжує систему числення залишкових класів, яка представляє коди поля Галуа у *k*-мірному просторі. Теоретичні основи системи залишкових класів глибоко досліджувались Николайчуком Я.М [5].

Теоретичною основою цілочисельного перетворення системи залишкових класів є доведення існування в кільці набору сукупності елементів $y_1, y_2 \ldots y_j \ldots, y_k$, які задовольняють систему Діофантових рівнянь:

$$\left.\begin{array}{c} y_j \equiv 1(\mathrm{mod}\, A_j) \\ y_j \equiv 0(\mathrm{mod} \prod^{k} A_j), \forall_j = \overline{1,k} \end{array}\right\}, \tag{1}$$

де $A_j$ - символ ідеалу причому

$$A_j + \prod_{i \neq j}^{k} A_i = A; \forall_j = \overline{1,k}. \tag{2}$$

В системі залишкових класів елементи $Y_j$ позначається через $B_j$ і називаються ортогональними базисами. При цьому $\{B_j\}$ повинні задовольняти систему рівнянь

$$\left.\begin{array}{c} \sum_{j=1}^{k} B_j \equiv 1(\mathrm{mod} \prod_{j=1}^{k} P_j) \\ B_j \equiv 1(\mathrm{mod}\, P_j) \end{array}\right\}, \tag{3}$$

де $P_j$ -попарно взаємно прості модулі, звідки слідує, що:

$$\left.\begin{array}{c} B_j \equiv 1(\mathrm{mod} \prod_{j-1}^{k} P_j) \\ B_j \equiv A(\mathrm{mod}\, P_j), i \neq j, \forall = \overline{1,k} \end{array}\right\}. \tag{4}$$

Це рішення означає, що кожне $B_j$ ділиться без остачі на всі $P_i$, якщо $i \equiv j$ і кожне $B_j$ ділиться без остачі на добуток $P_j$, тобто

$$B_j = m_j \prod_{i \neq j}^{k} P_i, \tag{5}$$

де $m_j$ - деяке ціле число у діапазоні $1 \leq m_j \leq P_j - 1$.

При цьому діапазон однозначного представлення чисел $N_j$ у цілочисельних системах залишкових класів знаходиться у межах

$$0 \le N_j \le \prod_{j=1}^{k} P_j - 1. \tag{6}$$

Якщо позначити

$$P = \prod_{j=1}^{k} P_j \text{, то } B_j = m_j \frac{P}{P_j}, \tag{7}$$

а $m_j$ може бути знайдено з рішення Діофантового рівняння

$$m_j \frac{P}{P_j} \equiv 1 (\mathrm{mod}\, P). \tag{8}$$

Визначенні теоретичні положення визначають пару перетворень цілочисельної системи залишкових класів у вигляді зворотнього

$$N_j = res \sum_{j=1}^{k} b_j B_j (\mathrm{mod}\, P) \tag{9}$$

та прямого перетворення

$$b_j = res N_k (\mathrm{mod}\, P_j); \forall_j = \overline{1,k}, \tag{10}$$

де $b_j$ - найменший невід'ємний залишок числа $N_j$ по модулю $P_j$, тобто $1 \le b_j \le P_j - 1$.

Традиційною галуззю застосування такого класу кодів Галуа та цілочисельної форми системи залишкових класів є побудова високопродуктивних процесорів, які працюють у модульній арифметиці системи залишкових класів.

Особливістю такої арифметики є відсутність наскрізних переносів, які існують у двійковій системі числення базису Радемахера. Тобто: додавання виконується згідно наступного виразу:

$$\begin{array}{l} x = (a_1, a_2, ..., a_j, ..., a_k) \\ y = (b_1, b_2, ..., b_j, ..., b_k) \\ \hline z = (c_1, c_2, ..., c_j, ..., c_k) \end{array}, \tag{11}$$

де $c_j = res(a_j + b_j) \bmod P_j; j \in \overline{1,k}$ [5].

Малорозрядність оброблюваних залишків дозволяє для підвищення швидкодії арифметичних операцій у обчислювальних каналах застосовувати методи табличної підстановки, а операції додавання та множення у системі залишкових класів (СЗК) здійснювати паралельно по $k$ обчислювальним каналам. Узагальнена структура пристроїв цифрової обробки сигналів у модулярній арифметиці представлена на рис.2

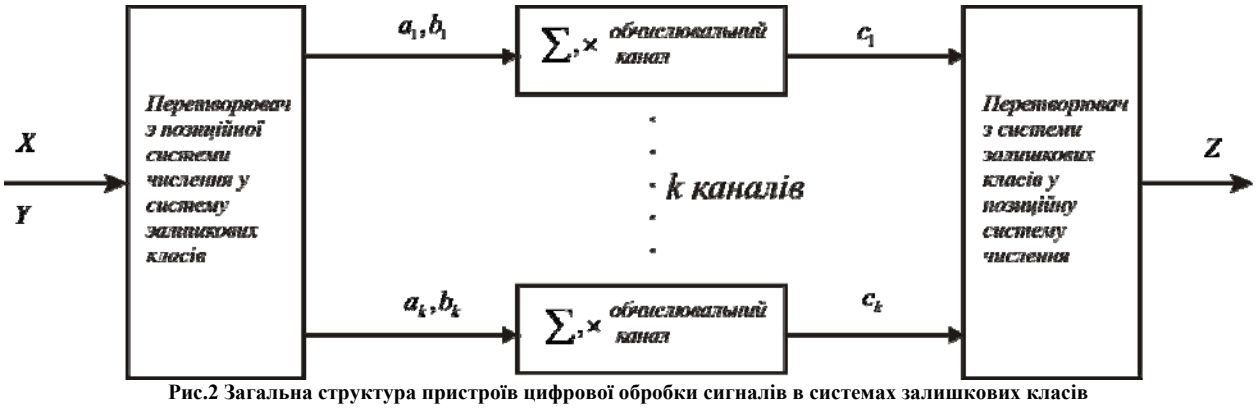


**Рис.2 Загальна структура пристроїв цифрової обробки сигналів в системах залишкових класів**

Структура наведена на рис.2 має цілий ряд преваг під час її реалізації на інтегральних схемах:

1. Незалежність кожного каналу забезпечує значну гнучкість під час планування і топологічного проектування кристалу мікросхеми

2. Реалізація таких пристроїв на основі ПЛІС, які мають обмежений вентильний ресурс, може бути легко оптимізована з точки зору розміщення функціональних блоків

3. Міжз'єднання трасування розташовуються лише всередині окремого обчислювального каналу, що виключає існування довгих трас, і як наслідок, це забезпечує деяке зменшення споживаної потужності і зменшення затримок проходження сигналів критичними шляхами

4. Відсутність спеціальних вимог по синхронізації між окремими каналами (окрім синхронізації входу та виходу) значно полегшує трасування кіл тактової частоти, що приводить до покращення такого параметру як джитер вихідного сигналу

5. За необхідності можливе введення додаткових надлишкових каналів для побудови відмово стійких систем.

Наведені факти, поряд із перевагами медулярних обчислювачів в швидкодії та площі кристалу, дозволяють говорити про обчислення в системах залишкових класів як про перспективу технологію високопродуктивних систем цифрової обробки сигналів, а особливо систем прямого цифрового синтезу.

Оскільки в системах залишкових класів (СЗК) використовуються модулярні операції, для високої ефективності необхідно використовувати спеціально спроектовані для СЗК суматори і помножувачі. Існує досить велика кількість підходів до реалізації суматорів за модулем m [6]. Далі будуть розглянуті найбільш типові і прості схеми модулярного підсумовування (рис. 3).

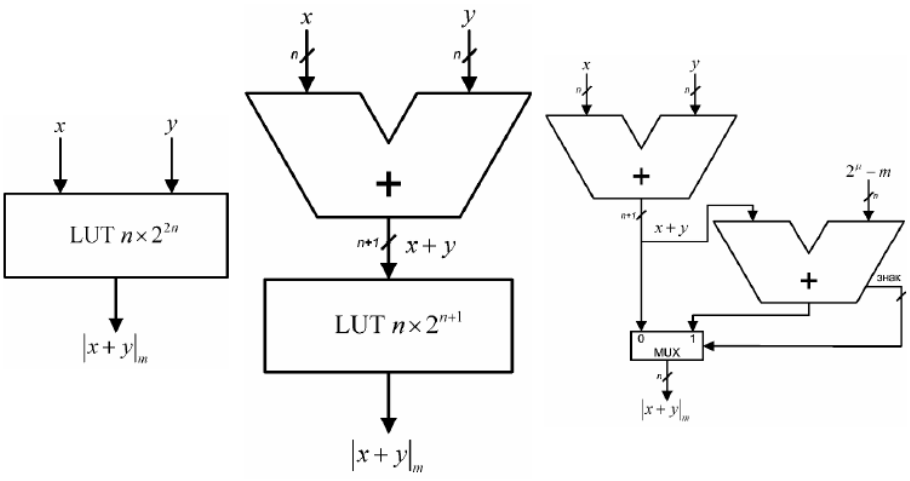


**Рис.3. Модулярне сумування . (а) – за допомогою великої LUT таблиці; (б) – з попереднім звичайним сумуванням ; (в) – без використання LUT таблиці,**

Перша з схем (рис.3.а) обчислює модулярну суму $|x+y|_m$ за допомогою таблиці розміром $n\times 2^{2n}, n=\lceil \log_2(m) \rceil$. Для двох відповідних елементів просто вибирається відповідь із великої таблиці. Таке рішення добре підходить для випадків, коли довжина слова мала, наприклад, $n \le 4$.

Для більших модулів, пам'ять LUT може набувати значних розмірів і тому інші схеми для підсумовування виявляються у цьому випадку більш раціональним. Структура (б) засновується на звичайному підсумовуванні $x+y$ та однієї таблиці, яка містить усі можливі значення для $|x+y|_m$. При цьому відчутно скорочуються розміри таблиці підстановки з $n\times 2^{2n}$ до $n\times 2^{n+1}$.

Третя схема (в) підсумовування є самою поширеною. У ній використовуються два суматора і мультиплексом для вибору результату у відповідності з виразом:

$$|x+y|_m = \begin{cases} x+y & 0 \le x+y < m \\ x+y-m & m \le x+y \end{cases} \qquad (12)$$

**Висновки**

Отже, переваги реалізації синтезаторів прямого цифрового синтезу (DDS) у кінцевих полях досягається заміною суматорів (а у деяких випадках перемножувачів) еквівалентними схемами, котрі за певних умов дозволять значно зекономити апаратні ресурси і реалізувати синтезатори з покращеними параметрами. Зокрема, при реалізації на ПЛІС замість апаратних перемножувачів і суматорів використовуються структури, які можуть будуватись на базі пам'яті типу ROM (Read Only Memory). Вартість такої пам'яті на порядок меша ніж вартість програмованої логічної інтегральної схеми.

**Література**

1. Макаренко В. Компоненты для построения беспроводных устройств святи. Часть 7. Синтезаторы частоты прямого цифровогосинтеза//Эдектронные компоненты и системы.-2010.-№1.-С.34-46

2. J.Vankka Direct Digital Synthesizers:Theory, Design and Applications, Helsinki University of Technology, 2000

3. Полікаровських О.І Архітектура прямого цифрового синтезатора частоти для рішень цифрового радіо/Полікаровських О.І. //Вісник Хмельницького національного університету.-2012. – №3. – С.142-146

4. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов/ Блейхут Р. – М.Мир, 1989

5. Николайчук Я.М Коди поля Галуа: теорія та застосування / Николайчук Я.М – Тернопіль: ТзОВ «Терно граф», 2012.-576 с.

6. Червяков Н.И. Принципы построения модулярных сумматоров и умножителей/ Червяков Н.И., Дяченко И.В.//Сборник научных трудов Ставропольского государственного университета.- 2006.-№1.-С.26-39.

**References**

1. Makarenko V. Komponenty dlja postroenija besprovodnyh ustrojstv svjati. Chast' 7. Sintezatory chastoty prjamogo cifrovogosinteza//Jedektronnye komponenty i sistemy.-2010.-№1.-S.34-46
2. J.Vankka Direct Digital Synthesizers:Theory, Design and Applications, Helsinki University of Technology, 2000
3. Polikarovs'kih O.I Arhitektura prjamogo cifrovogo sintezatora chastoti dlja rishen' cifrovogo radio/Polikarovs'kih O.I. //Visnik Hmel'nic'kogo nacional'nogo universitetu.-2012. – №3.-S.142-146
4. Blejhut R. Bystrye algoritmy cifrovoj obrabotki signalov/ Blejhut R. – M. Mir, 1989
5. Nikolajchuk Ja.M Kodi polja Galua: teorija ta zastosuvannja / Nikolajchuk Ja.M – Ternopil': TzOV «Ternograf», 2012.-576 s.
6. Chervjakov N.I. Principy postroenija moduljarnyh summatorov i umnozhitelej/ Chervjakov N.I., Djachenko I.V.//Sbornik nauchnyh trudov Stavropol'skogo gosudarstvennogo universiteta.- 2006.-№1.-S.26-39.

Рецензія/Peer review : 8.11.2013 р. Надрукована/Printed :23.11.2013 р.
Рецензент: Параска Г.Б., д.т.н., проф.



## Повні вимоги до оформлення рукопису http://visniktup.narod.ru/rules/

**Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 3 від 27.11.2013 р.**

Підп. до друку 26.11.2009 р. Ум.друк.арк. 18,26 Обл.-вид.арк. 22,65
Формат 30х42/4, папір офсетний. Друк різографією.
Наклад 100, зам. № _____

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу "Вісник Хмельницького національного університету"
редакційно-видавничим центром Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1. тел (0382) 72-83-63