

# РАДИОЕЛЕКТРОНИКА ТА ТЕЛЕКОМУНІКАЦІЇ

## RADIO ELECTRONICS AND TELECOMMUNICATIONS

### РАДИОЭЛЕКТРОНИКА И ТЕЛЕКОММУНИКАЦИИ

УДК 621.391

#### АЛГОРИТМИ ПОШУКУ ПЕРІОДИЧНОСТЕЙ У ЦИФРОВИХ ПОСЛІДОВНОСТЯХ З БЛОКОВИМ КОДУВАННЯМ ЗА ЇХ КОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

**Романов О. М.** – канд. техн. наук, заступник начальника з наукової роботи, науково-дослідний інститут Міністерства оборони України, Київ, Україна.

**Котюбін В. Ю.** – науковий співробітник, науково-дослідний інститут Міністерства оборони України, Київ, Україна.

#### АНОТАЦІЯ

**Актуальність** Для підвищення завадостійкості систем зв'язку і передачі даних широко застосовується завадостійке кодування. Найбільш розповсюдженими через свою ефективність є методи блокового кодування. В умовах часткової апріорної невизначеності виду і параметрів кодування перед декодуванням цифрової послідовності проводиться попередній аналіз для їх визначення. При блоковому кодуванні для визначення періоду цифрової послідовності, обумовленого додаванням до неї синхропослідовності, і який може визначати вид і параметри кодування, розповсюдженим підходом є використання їх кореляційних властивостей.

**Метою** роботи є викладення алгоритмів пошуку періодичностей у цифрових послідовностях з блоковим завадостійким кодуванням в умовах часткової апріорної невизначеності виду і параметрів завадостійкого коду.

**Метод.** У статті наведено два алгоритми пошуку періодичностей у цифрових послідовностях з блоковим кодуванням та описано принцип їх роботи. В основі одного алгоритму лежить обчислення АКФ, в основі іншого – ВКФ. Показано, що довжина цифрової послідовності повинна бути щонайменше в два рази більше максимально можливого періоду. Роботу обох алгоритмів проілюстровано на прикладах.

**Результати.** На основі запропонованих алгоритмів розроблено СПЗ. Результати визначення періоду цифрових послідовностей з блоковим завадостійким кодуванням при різних значеннях періоду підтвердили працездатність запропонованих алгоритмів. Обидва запропоновані алгоритми дають приблизно однаковий результат. Встановлено експериментальні залежності часу обчислення АКФ і ВКФ від довжини цифрової послідовності і максимально можливого періоду. Алгоритм пошуку періоду цифрової послідовності за ВКФ її складових є більш ефективним через меншу кількість обчислень.

**Висновки.** У роботі вперше отримано два алгоритми пошуку періодичностей у цифрових послідовностях з блоковим завадостійким кодуванням, які засновані на визначенні їх кореляційних функцій. Застосування розроблених алгоритмів на практиці дає змогу в умовах часткової апріорної невизначеності виду і параметрів завадостійкого коду визначати період цифрових послідовностей у масштабі реального часу навіть при великих значеннях періоду, а на його основі – ідентифікувати вид і параметри блокових завадостійких кодів.

**КЛЮЧОВІ СЛОВА:** автокореляційна функція, взаємна кореляційна функція, цифрова послідовність, період, блоковий завадостійкий код, синхропослідовність, система зв'язку і передачі даних.

#### АБРЕВІАТУРИ

LDPC – low-density parity-check;  
TPC – turbo product code;  
АКФ – автокореляційна функція;  
ВКФ – взаємна кореляційна функція;  
ЕОМ – електронно-обчислювальна машина;  
ЗК – завадостійкий код;  
СЗПД – система зв'язку і передачі даних;

СП – синхропослідовність;  
СПЗ – спеціальне програмне забезпечення;  
ЦП – цифрова послідовність.

#### НОМЕНКЛАТУРА

$e$  – кількість помилкових біт у СП ЦП  $s_1(n)$  та  $s_2(n)$ ;  
 $K$  – довжина СП у блоці;  
 $L$  – довжина прийнятої ЦП;

$l$  – довжина штучно утворених ЦП;  
 $L_{\min}$  – мінімально необхідна довжина ЦП;  
 $M$  – довжина перевірочних даних у блоці;  
 $N$  – довжина інформації у блоці;  
 $q$  – кількість блоків;  
 $R$  – кількість одиниць у  $\tau$  комірці масиву  $R(\tau)$ ;  
 $R(\tau)$  – АКФ ЦП;  
 $R_{12}(l)$  – ВКФ ЦП;  
 $s(n)$  – ЦП;  
 $s_1(n)$  – перша ЦП, штучно утворена з  $s(n)$ ;  
 $s_2(n)$  – друга ЦП, штучно утворена з  $s(n)$ ;  
 $s_p(n)$  – результуюча ЦП;  
 $T$  – період ЦП;  
 $T_{\min}$  – мінімально можливий період ЦП;  
 $T_{\max}$  – максимально можливий період ЦП;  
 $\Delta_{СП}$  – величина зсуву СП від початку ЦП;  
 $\tau$  – затримка ЦП у часі;  
 $\equiv$  – оператор логічної операції «еквівалентність».

### ВСТУП

У СЗПД, які набули широкого розповсюдження, використовуються різноманітні методи, протоколи, стандарти передачі даних. Для підвищення ймовірності правильного прийому дані піддаються попередньому ЗК [1]. Найбільш розповсюдженими через свою ефективність [2] видами ЗК у сучасних СЗПД є згорткове кодування, кодування Ріда-Соломона, складені коди, TRC та LDPC коди [3–5]. Більшість ЗК, що використовуються практично, є блоковими.

Для декодування прийнятих даних за існуючими методами, алгоритмами, стандартами повинні бути відомі вид і параметри коду [1]. В умовах часткової апіорної невизначеності виду і параметрів кодування необхідно попередньо провести аналіз ЦП для їх визначення [5]. Розвитку методичного апарату аналізу ЦП, який проводиться перед декодуванням, приділяється значно менша увага [6].

Для синхронізації декодера блокових кодів перед кодованим блоком даних вставляється СП, яка обумовлює періодичність ЦП [3, 7]. На цьому заснований принцип дії методів визначення виду і параметрів ЗК [5]. Недоліки, притаманні практичним реалізаціям останніх [8, 9], обмежують їх застосування. Отже, актуальним є дослідження алгоритмів визначення виду і параметрів блокових ЗК, зокрема, алгоритмів пошуку періодичностей.

**Об'єктом дослідження** є процес визначення періоду ЦП даних з блоковим ЗК.

**Предметом дослідження** є алгоритми пошуку періоду ЦП даних з блоковим ЗК.

**Метою роботи** є викладення алгоритмів пошуку періодичностей у ЦП з блоковим ЗК в умовах часткової апіорної невизначеності параметрів ЗК та дослідження їх ефективності.

### 1 ПОСТАНОВКА ЗАДАЧІ

Нехай перед передаванням ЦП  $s(n)$  розбивається на  $q$  блоків однакової довжини  $N$  біт. До кожного

блока ЦП додаються перевірочні дані довжиною  $M$  біт [1]. Для синхронізації декодера з початком блоків перед кожним блоком вставляється СП довжиною  $K$  біт. Період  $T$  такої ЦП визначається:  $T=N+M+K$  біт, а сама послідовність може бути представлена схематично, як показано на рис. 1.

У сформованій таким чином ЦП  $K$  біт СП постійні для кожного з  $q$  блоків. Решта  $N+M$  біт є статистично незалежними.

Необхідно визначити період  $T$  прийнятої ЦП  $s(n)$ .

### 2 ОГЛЯД ЛІТЕРАТУРИ

Аналіз останніх досліджень і публікацій показує, що найбільш розповсюдженим методом виявлення періодичностей у сигналах є аналіз їх кореляційних властивостей. Найбільшого поширення кореляційна функція набула в системах радіолокації [10–12], а також знайшла своє застосування у додатках цифрової обробки сигналів [13, 14].

Аналізу ЦП даних методами кореляційної обробки присвячені роботи [8, 9]. До недоліків алгоритмів, отриманих авторами, слід віднести необхідність проведення великої кількості обчислень для розпізнавання блокових кодів довжиною більше 255 біт [8], а також проведення обчислень і розпізнавання блокових кодів тільки в масштабі нереального часу [9], що є неприйнятним для практичного застосування.

### 3 МАТЕРІАЛИ І МЕТОДИ

Для пошуку періоду ЦП розроблено два алгоритми. Розглянемо перший з них, який базується на основі обчислення АКФ ЦП.

Для отримання інформації про період  $T$  прийнятої детермінованої ЦП довжиною  $L$  біт як дійсної функції часу використаємо її АКФ [7, 8]:

$$R(\tau) = \frac{1}{L} \sum_{n=0}^{L-1} s(n)s(n+\tau). \quad (1)$$

Під операцією множення для бінарної ЦП будемо розуміти логічну операцію «еквівалентність», таблиця істинності для якої представлена в табл. 1.

Таблиця 1 – Таблиця істинності для операції «еквівалентність»

$s_1$	$s_2$	$s_1 \equiv s_2$
“1”	“1”	“1”
“1”	“0”	“0”
“0”	“1”	“0”
“0”	“0”	“1”

Операція дає істинний результат при однакових значеннях елементів, над якими виконується. Тоді (1) набуває виду:

$$R(\tau) = \frac{1}{L} \sum_{n=0}^{L-1} s(n) \equiv s(n+\tau). \quad (2)$$

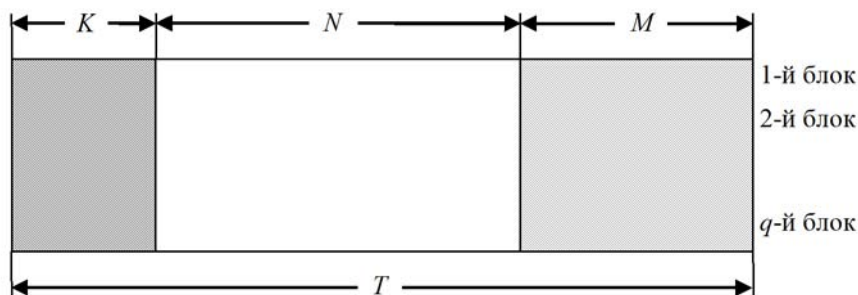


Рисунок 1 – Цифрова послідовність з періодом повторення  $T$

Приклад обчислення АКФ двох фрагментів ЦП за формулою (2) представлений на рис. 2.

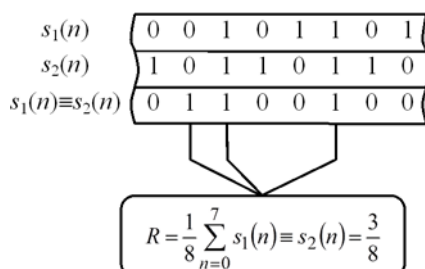


Рисунок 2 – Приклад обчислення АКФ

За відсутності зсуву ( $\tau=0$ ) дві ЦП  $s(n)$  будуть повністю ідентичними, що обумовить локальний максимум АКФ  $R(0)$ , значення якого дорівнює одиниці:

$$R(0) = \frac{1}{L} \sum_{n=0}^{L-1} s(n) \equiv s(n) = \frac{L}{L} = 1.$$

При  $\tau \neq 0$  АКФ набуватиме максимуму при співпадіннях СП, що відповідає періоду  $T$  ЦП. Для його відшукування передбачимо можливість введення мінімально  $T_{\min}$  і максимально можливого періоду  $T_{\max}$  залежно від апріорно відомих даних. В більшості випадків доцільно покласти  $T_{\min}=0$ .

Визначимо мінімально необхідну довжину  $L_{\min}$  ЦП  $s(n)$  для успішного відшукування періоду  $T$ .

Для цього спочатку розглянемо випадок синхронізації ЦП на початок СП (рис. 3). Як показано вище, за

відсутності зсуву ЦП (рис. 3а) спостерігатиметься локальний максимум АКФ.

При поступовому зсуванні ЦП ( $\tau > 0$ ) через статистичну незалежність її елементів АКФ буде мати близьке до постійного значення, менше за максимальне (рис. 3б), і досягне локального максимуму при  $\tau=T$  через ідентичність другої СП ЦП  $s(n)$  і першої СП ЦП  $s(n+\tau)$  (рис. 3в). Отже, в цьому випадку для відшукування періоду  $T$  ЦП достатньо її довжини  $L_{\min}=T+K=2K+N+M$ .

В умовах апріорної невизначеності виду і параметрів ЗК ЦП не синхронізована на початок СП (рис. 4), що обумовлює необхідність збільшення її мінімальної довжини на величину зсуву СП  $\Delta_{СП}$  від початку:  $L_{\min}=T+K+\Delta_{СП}=2K+N+M+\Delta_{СП}$ .

Найбільш «жорстким» варіантом зсуву СП є її розрив із залишком на початку ЦП  $K-1$  біт СП (рис. 5). У такому випадку для забезпечення співпадіння  $K$  біт СП ЦП, зсунутих між собою на  $\tau=T$ , їх довжина повинна бути не менше  $L_{\min}=2T$ .

Із порівняння отриманих значень мінімальної довжини ЦП для випадків синхронізації ЦП, наведених на рис. 3–5, видно, що в умовах апріорної невизначеності виду і параметрів ЗК мінімальна довжина ЦП повинна бути не менше подвоєного значення максимально можливого періоду ЦП  $L_{\min}=2T_{\max}$ .

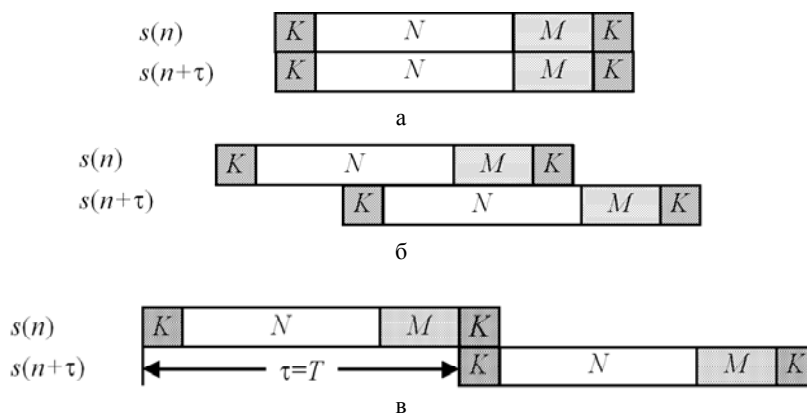


Рисунок 3 – Ілюстрація алгоритму пошуку за АКФ періоду ЦП, синхронізованої на початок СП:  
 а –  $\tau=0$ ; б –  $0 < \tau < T$ ; в –  $\tau=T$

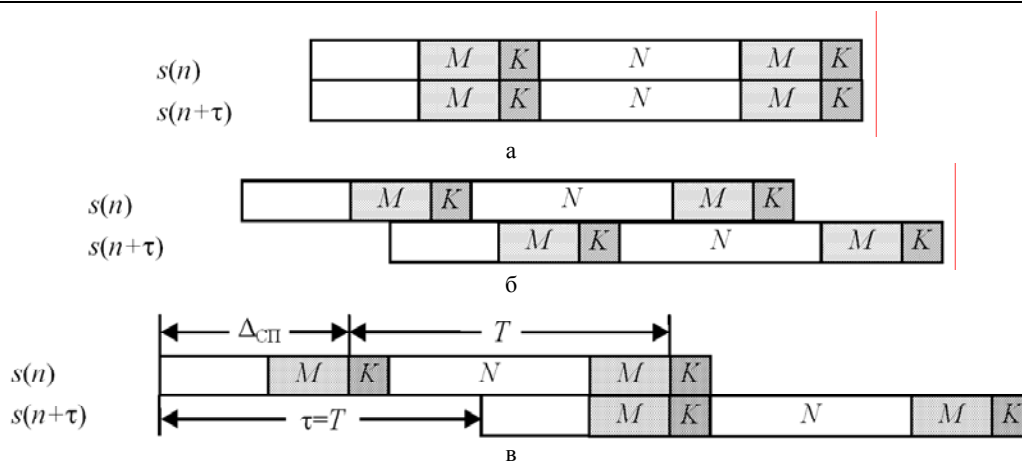


Рисунок 4 – Ілюстрація алгоритму пошуку за АКФ періоду ЦП, не синхронізованої на початок СП: а –  $\tau=0$ ; б –  $0 < \tau < T$ ; в –  $\tau=T$

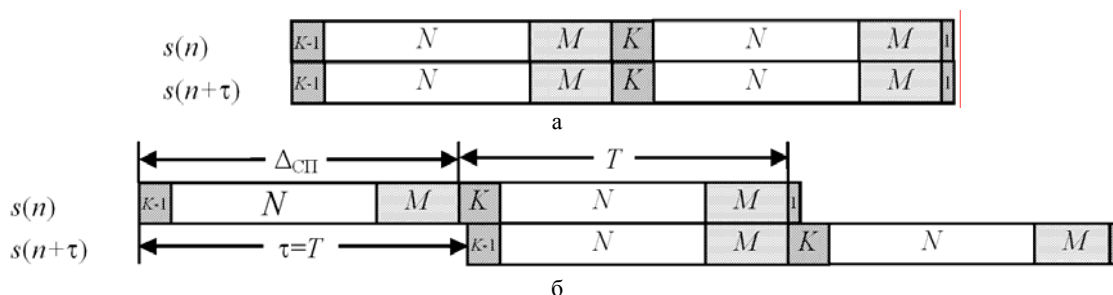


Рисунок 5 – Ілюстрація алгоритму пошуку за АКФ періоду ЦП із розривом СП: а –  $\tau=0$ ; б –  $\tau=T$

Суть алгоритму пошуку періоду полягає у зсуві другої ЦП відносно першої вправо з кроком один біт від  $\tau=T_{\min}$  до  $\tau=T_{\max}$  (рис. 3б, 4б). На кожному кроці зсуву над ними побітно виконується логічна операція «еквівалентність»:  $s_p(n)=s(n)\equiv s(n+\tau)$ . У  $\tau$  комірці результуючого масиву  $R(\tau)$  кількість одиниць  $R$  відповідає кількості біт, що співпали.

Очевидно, що при  $\tau=0$  операція «еквівалентність» виконується над  $L$  біт ЦП. Із кожним кроком збільшення  $\tau$  кількість пар елементів ЦП  $s(n)$  і  $s(n+\tau)$ , над якими виконується операція «еквівалентність», зменшується на  $\tau$ . Тому для корегування крайового ефекту, який при цьому виникає [13], модифікуємо формулу обчислення АКФ (2):

$$R(\tau) = \frac{1}{L-\tau} \sum_{n=\tau}^{L-1} s(n) \equiv s(n+\tau). \quad (3)$$

У формулі (3) операція «еквівалентність» і нормування здійснюються по кількості пар елементів ЦП, по яким реально обчислюється АКФ.

В отриманій описаним способом АКФ відшукуються максимальні значення  $\max[R(\tau)]$ . Найменше  $\tau$ ,  $0 < \tau \leq T_{\max}$ , при якому функція  $R(\tau)$  набуває максимуму, відповідає періоду  $T$  ЦП. Решта значень  $\tau$ , при яких  $R(\tau)$  набуває максимуму, відповідають кратним значенням періоду ЦП:  $2T, 3T \dots$

Алгоритм пошуку періодичності ЦП за АКФ, що відображає описану послідовність дій, представлений на рис. 6. Результат пошуку періоду ЦП за наведеним алгоритмом представлений на рис. 9.

Для реалізації другого алгоритму пошуку періодичності у прийнятій ЦП  $s(n)$  довжиною  $L$  за ВКФ штучно утворимо з неї дві ЦП  $s_1(n)$  і  $s_2(n)$ , між якими шукатимемо кореляцію. Перша ЦП  $s_1(n)$ , довжиною  $l=T_{\min}$ , – від початку  $s(n)$  до значення мінімально можливого періоду  $T_{\min}$ . Друга ЦП  $s_2(n)$  – від значення  $T_{\min}+1$  ЦП  $s(n)$ , також довжиною  $l$  (рис. 7):  $s_1(n)=s(0 \dots T_{\min}-1)$ ;  $s_2(n)=s(T_{\min} \dots 2T_{\min}-1)$ .

Обчислимо значення ВКФ між утвореними ЦП [13]:

$$R_{12}(l) = \frac{1}{l} \sum_{n=0}^{l-1} s_1(n) \equiv s_2(n). \quad (4)$$

Для цього, як і в попередньому алгоритмі, побітно виконуватимемо логічну операцію «еквівалентність»:  $s_p(n)=s_1(n)\equiv s_2(n)$ . В результаті її виконання «одиниця» отримується за умови еквівалентності бітів. Отримана кількість одиниць підраховується із застосуванням оператора  $\sum$  і нормується до загальної кількості біт  $l$  у ЦП.

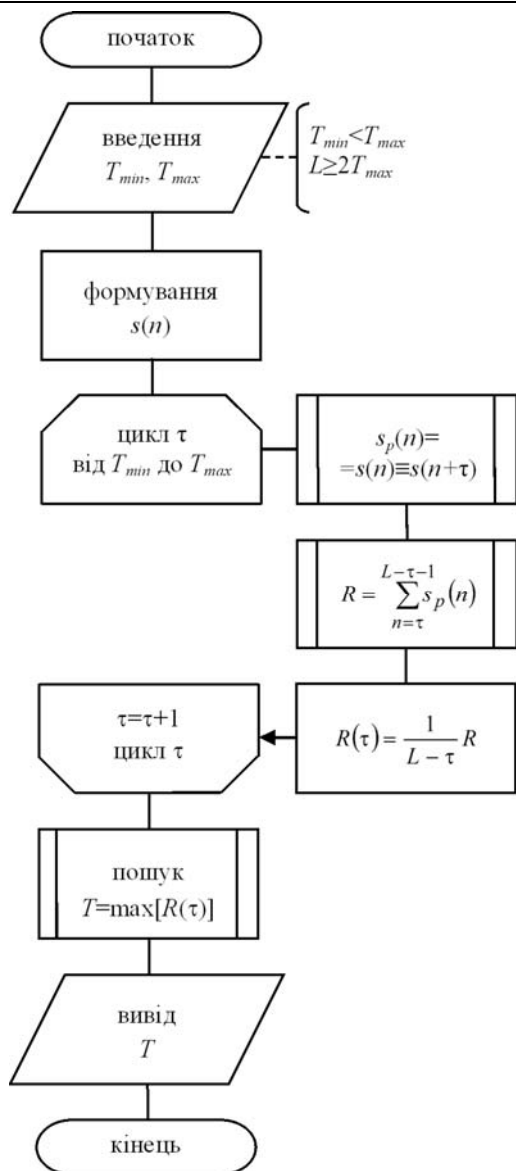


Рисунок 6 – Алгоритм пошуку періодичності ЦП за АКФ

Із кроком один біт збільшуватимемо  $l$  від значення  $T_{\min}$  до максимально можливого значення періоду  $T_{\max}$ , зсуваючи при цьому на відповідну кількість біт початок ЦП  $s_2(n)$ . На кожному кроці обчислюватимемо ВКФ ЦП. Через статистичну незалежність елементів ЦП значення ВКФ буде значно меншим порівняно із величинами локальних максимумів ВКФ (рис. 7б–ж). При досягненні довжини сформованих ЦП  $l$  значення істинного періоду  $T$  ЦП, що аналізується, зсув СП у  $s_1(n)$  та  $s_2(n)$  від їх початку буде однаковим (рис. 7з), що обумовить різке збільшення кількості біт, що співпадають між  $s_1(n)$  та  $s_2(n)$ , і сплеск їх ВКФ. Подальше збільшення довжини сформованих ЦП призведе до циклічної появи сплесків ВКФ при співпадіннях другої та послідовних СП. Отже, істинне значення періоду ЦП  $T$  відповідає першому максимуму ВКФ і може бути підтверджене появою максимумів ВКФ на кратних періодах  $2T, 3T \dots$ . Максимальне значення періоду  $T_{\max}$  не може перевищувати цілої

частини від половини довжини прийнятої ЦП, що аналізується:  $T_{\max} \leq L/2$ . І навпаки: для відшукування періоду ЦП за ВКФ довжина ЦП  $L$  має бути такою, щоб в ній містилося не менше двох СП:  $L \geq 2T_{\max}$ .

Алгоритм пошуку періоду ЦП за ВКФ її складових, що відображає описану послідовність дій, представлений на рис. 8.

Результат пошуку періоду ЦП за наведеним алгоритмом представлений на рис. 10.

Принциповою відмінністю цього алгоритму від попереднього є пошук кореляційних властивостей різних ЦП, що слідують одна за одною у часі.

В обох розглянутих алгоритмах в загальному випадку крок зсуву може бути відмінним від одиниці.

Ймовірність появи помилкового біту в СП однієї з ЦП обумовлює зменшення обчисленої кореляційної функції при вірному періоді на  $e/l$ , де  $e$  – кількість помилкових біт у СП.

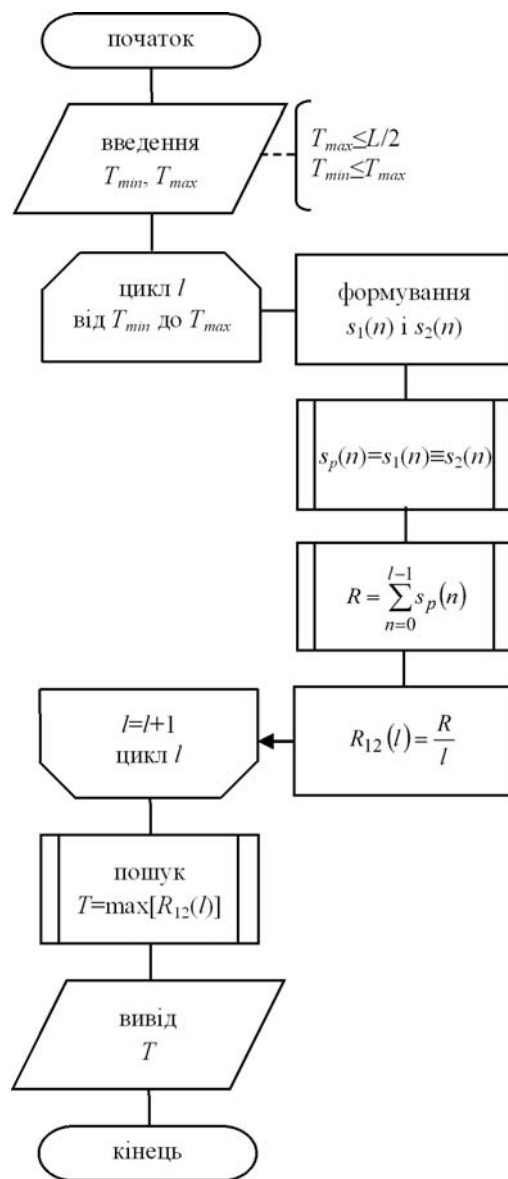


Рисунок 8 – Алгоритм пошуку періодичності ЦП за ВКФ її складових

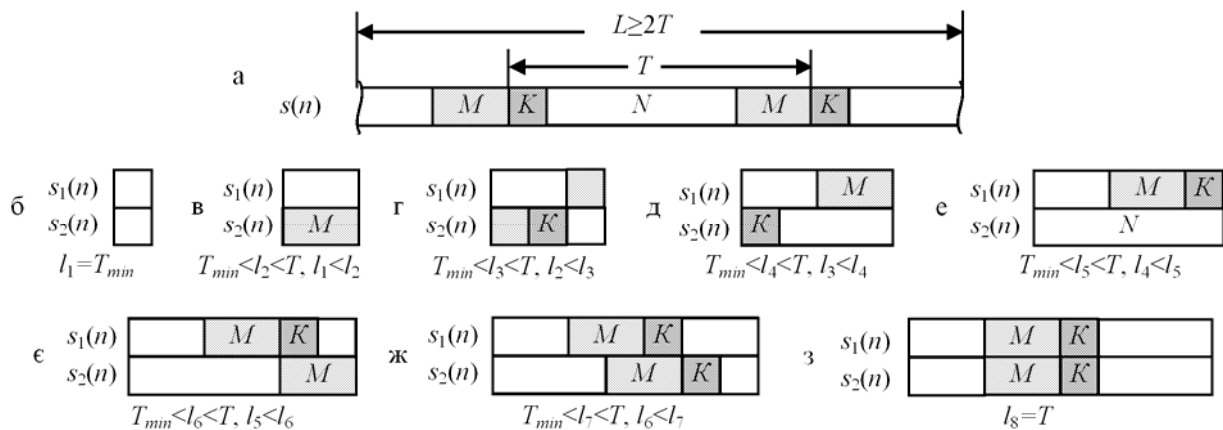


Рисунок 7 – Ілюстрація алгоритму пошуку періоду ЦП за ВКФ її складових:

а – вхідна ЦП; б-з – штучно утворені ЦП

#### 4 ЕКСПЕРИМЕНТИ

Для визначення ефективності роботи запропонованих алгоритмів у Visual Studio 2019 мовою програмування C# розроблено СПЗ з підтримкою паралельних обчислень на багатоядерних центральних процесорах. Експерименти проводились на ЕОМ з 64-розрядною операційною системою Windows 10 і такими параметрами:

- двоядерний центральний процесор Intel Core 2 Duo E6700 з тактовою частотою 2,66 ГГц із 4 ГБ пам'яті;

- чотириядерний центральний процесор Intel Core i5-4460 з тактовою частотою 3,2 ГГц із 8 ГБ пам'яті;

- чотириядерний восьмипоточковий центральний процесор Intel Core i7-4790K з тактовою частотою 4 ГГц із 8 ГБ пам'яті.

У всіх експериментах задавалось:  $T_{min}=0$ ,  $\tau=1$  ( $\Delta l=1$ ),  $L = 2000, 4000, 8000, 16000, 32000, 48000, 64000, 80000, 96000, 112000, 128000$  біт. Значення  $T_{max}$  задавалось у межах від 1000 біт до  $L/2$  (для ЦП з найбільшою довжиною  $L=128000$  біт  $T_{max}$  становило 64000 біт), тобто від суттєво меншого за довжину ЦП до максимального.

Період ЦП визначався за обома описаними алгоритмами і вимірювався час його визначення без врахування введення і виведення даних та пошуку максимального значення у результуючому масиві  $R(\tau)$  ( $R(l)$ ).

При проведенні експериментів використовувалися реальні ЦП з телекомунікаційних мереж, ймовірність помилки у яких знаходилась у межах  $10^{-5}$ – $10^{-6}$ . За такої ймовірності помилки кількість помилок у всій ЦП довжиною від 2000 до 128000 біт не перевищувала одну, що дає змогу вважати ЦП безпомилковими (ідеальними).

#### 5 РЕЗУЛЬТАТИ

АКФ і ВКФ, обчислені за розробленими в роботі алгоритмами, для ЦП із періодом 1504 біт представлені на рис. 9, 10 відповідно.

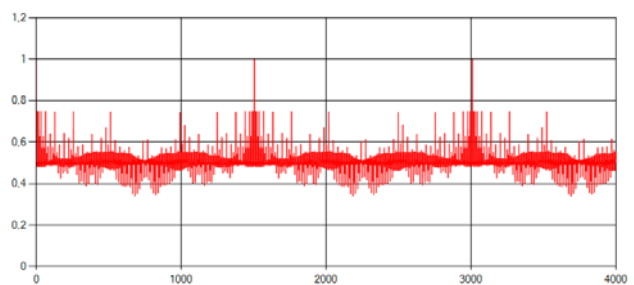


Рисунок 9 – Результати пошуку АКФ,  $T=1504$  біти

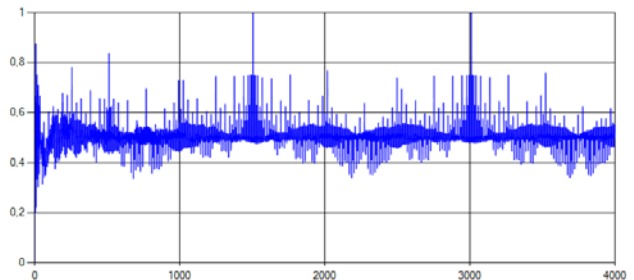


Рисунок 10 – Результати пошуку ВКФ,  $T=1504$  біти

На рис. 11, 12 представлені результати обчислення АКФ ЦП довжиною  $L=20000$  біт, істинний період якої становить  $T=424$  біти. Рис. 11 відповідає пошуку АКФ при заданому максимальному для даної довжини ЦП  $T_{max}=L/2=10000$  біт. Рис. 12 відповідає пошуку АКФ при  $T_{max}=500$ , який незначно перевищує  $T$ .

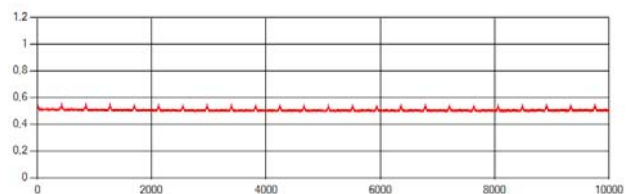


Рисунок 11 – Результати пошуку АКФ,  $T_{max}=10000$  біт

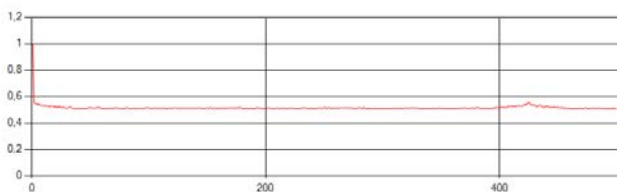


Рисунок 12 – Результати пошуку АКФ,  $T_{max}=500$  біт

Час обчислення за запропонованими алгоритмами АКФ, представлений у табл. 2, а ВКФ – у табл. 3, 4. Отримані результати також представлені у вигляді графіків. Графік залежності часу обчислення АКФ від довжини ЦП при різних значеннях  $T_{max}$  представлений на рис. 13, а від  $T_{max}$  при різних значеннях  $L$  – на рис. 14. Графік залежності часу обчислення ВКФ від максимально можливого періоду  $T_{max}$  представлений на рис. 15.

Таблиця 2 – Час обчислення АКФ ЦП, с

$T_{max}$ , біт		$L$ , біт										
		2000	4000	8000	16000	32000	48000	64000	80000	96000	112000	128000
1000	Core 2	0,002	0,004	0,008	0,016	0,032	0,045	0,062	0,076	0,091	0,106	0,123
	Core i5	0,001	0,003	0,007	0,014	0,027	0,034	0,044	0,047	0,055	0,058	0,062
	Core i7	0,000	0,000	0,001	0,003	0,006	0,010	0,013	0,017	0,020	0,023	0,027
2000	Core 2		0,007	0,014	0,029	0,060	0,089	0,121	0,150	0,179	0,211	0,242
	Core i5		0,005	0,013	0,026	0,038	0,053	0,066	0,075	0,078	0,088	0,095
	Core i7		0,001	0,003	0,006	0,013	0,020	0,027	0,035	0,039	0,046	0,053
4000	Core 2			0,025	0,055	0,116	0,174	0,238	0,294	0,354	0,412	0,480
	Core i5			0,021	0,038	0,059	0,074	0,094	0,107	0,122	0,138	0,152
	Core i7			0,005	0,012	0,025	0,038	0,052	0,064	0,077	0,091	0,102
8000	Core 2				0,093	0,214	0,332	0,457	0,571	0,691	0,811	0,941
	Core i5				0,059	0,088	0,115	0,148	0,178	0,209	0,237	0,268
	Core i7				0,020	0,047	0,072	0,096	0,123	0,148	0,175	0,199
16000	Core 2					0,369	0,602	0,850	1,080	1,322	1,560	1,820
	Core i5					0,127	0,185	0,248	0,304	0,367	0,428	0,488
	Core i7					0,078	0,130	0,182	0,223	0,282	0,335	0,384
24000	Core 2						0,812	1,172	1,532	1,890	2,253	2,610
	Core i5						0,238	0,330	0,412	0,504	0,597	0,688
	Core i7						0,174	0,250	0,331	0,404	0,485	0,560
32000	Core 2							1,454	1,921	2,403	2,882	3,387
	Core i5							0,396	0,517	0,632	0,754	0,882
	Core i7							0,309	0,410	0,510	0,615	0,716
40000	Core 2								2,252	2,849	3,448	4,048
	Core i5								0,599	0,744	0,898	1,052
	Core i7								0,481	0,612	0,738	0,875
48000	Core 2									3,237	3,961	4,680
	Core i5									0,850	1,031	1,216
	Core i7									0,687	0,851	0,994
56000	Core 2										4,414	5,253
	Core i5										1,144	1,352
	Core i7										0,944	1,125
64000	Core 2											5,865
	Core i5											1,493
	Core i7											1,233

Таблиця 3 – Час обчислення ВКФ ЦП (ЕОМ з процесором Intel Core 2 Duo), с

$T_{max}$ , біт	$L$ , біт										
	2000	4000	8000	16000	32000	48000	64000	80000	96000	112000	128000
1000	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001
2000		0,002	0,002	0,002	0,002	0,002	0,002	0,002	0,002	0,002	0,002
4000			0,007	0,007	0,007	0,007	0,007	0,007	0,007	0,007	0,007
8000				0,026	0,026	0,026	0,026	0,026	0,026	0,026	0,026
16000					0,099	0,099	0,099	0,099	0,099	0,099	0,099
24000						0,222	0,222	0,222	0,222	0,222	0,222
32000							0,394	0,394	0,394	0,394	0,394
40000								0,613	0,613	0,613	0,613
48000									0,883	0,883	0,883
56000										1,195	1,195
64000											1,558

Таблиця 4 – Час обчислення ВКФ ЦП  $L=128000$  біт

Час обчислення, с	$T_{max}$ , біт										
	1000	2000	4000	8000	16000	24000	32000	40000	48000	56000	64000
Core i5	0,001	0,002	0,008	0,028	0,061	0,102	0,158	0,224	0,309	0,402	0,522
Core i7	0,000	0,000	0,001	0,006	0,027	0,058	0,102	0,162	0,237	0,316	0,411



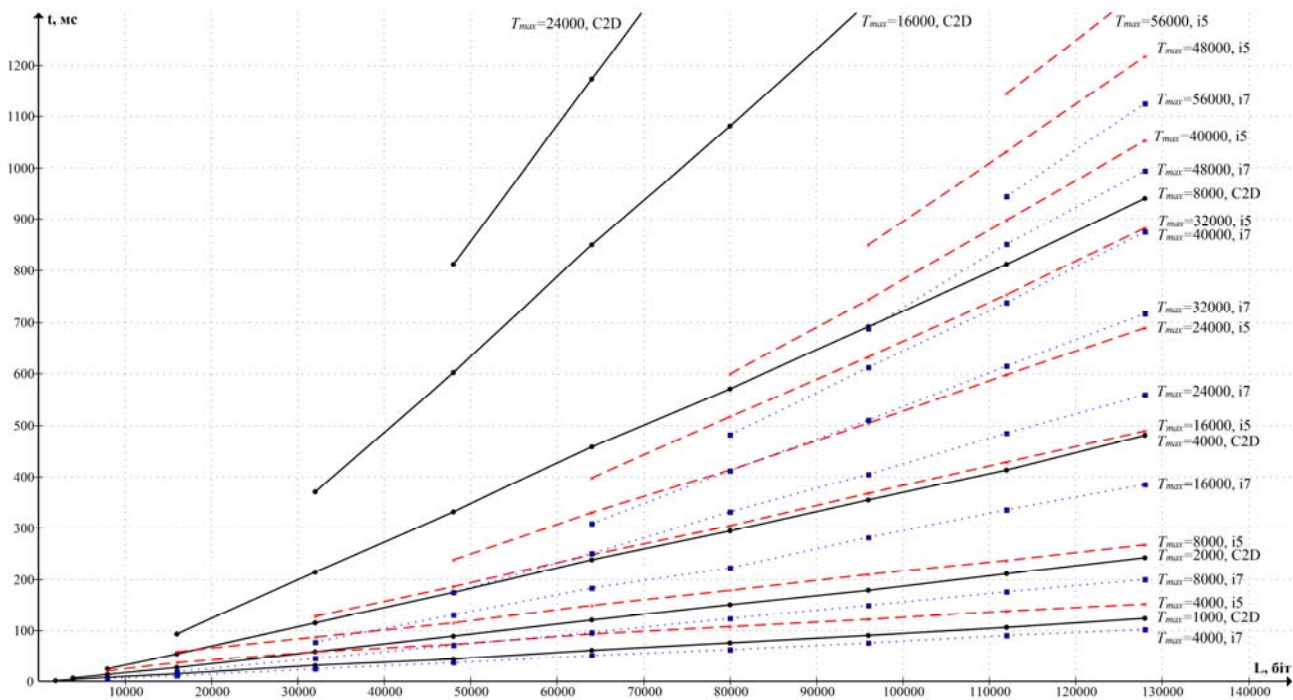


Рисунок 13 – Графік залежності часу обчислення АКФ від довжини ЦП  $L$

## 6 ОБГОВОРЕННЯ

Для більшості ЦП, що досліджувались, за обома розробленими алгоритмами в результаті кореляційних масивів  $R(\tau)$  ( $R(l)$ ) отримано максимальне значення, по якому вірно обчислено період ЦП. Винятком є ЦП з короткими СП, кореляція на довжині яких не забезпечує появу вираженого максимуму у результатуючому масиві  $R(\tau)$  ( $R(l)$ ). Наприклад, в СЗПД, організованій за стандартом [15], довжина СП становить менше 1% від періоду, чого не достатньо для отримання вираженого максимуму в кореляційному масиві. Тому у подальшому доцільно дослідити вплив довжини СП у ЦП (відношення  $K/T$ ) та її структури на величину максимумів кореляційних функцій. Також доцільно дослідити вплив шумів та завад на величину максимумів кореляційних функцій: із збільшенням ймовірності помилки у ЦП кількість біт СП, що співпали, зменшуватиметься, що, у свою чергу, призведе до зменшення максимумів АКФ і ВКФ.

На рис. 9, 10 видно максимуми кореляційних функцій, обумовлені співпадінням СП ЦП на періодах кореляції, кратних істинному. Також із порівняння рис. 9 і 10 видно, що результати обчислення АКФ і ВКФ однакові, за винятком початкової ділянки, на якій ВКФ обчислюється для дуже коротких ЦП, в той час як АКФ обчислюється для ЦП постійної довжини.

Із порівняння рис. 11, 12 видно, що алгоритм обчислення АКФ коректно працює як за умови  $T < T_{\max} \ll L$ , так і за умови  $T \ll T_{\max} = L/2$ . Другий випадок дозволяє отримати максимуми АКФ, які відпо-

відають кратним значенням періоду ЦП та дозволяють підтвердити визначений період.

Із порівняння табл. 2, 3 і 4 видно, що при однаковій довжині ЦП  $L$  і максимальному періоді  $T_{\max}$  час обчислення ВКФ в декілька разів (залежно від  $L$  і  $T_{\max}$ ) менше часу обчислення АКФ, що обумовлено меншою кількістю операцій «еквівалентність», які виконуються у кожному циклі.

Із табл. 2 і рис. 13 видно, що час обчислення АКФ знаходиться в лінійній залежності від довжини ЦП. Коефіцієнт пропорційності визначається значенням  $T_{\max}$ , параметрами ЕОМ та ефективністю програмної реалізації алгоритмів.

Також з табл. 2 і рис. 14 видно, що залежність часу обчислень АКФ від максимального періоду ЦП  $T_{\max}$  може бути описана поліномом другого ступеню, коефіцієнти якого визначаються довжиною ЦП, параметрами ЕОМ та ефективністю програмної реалізації алгоритмів. Зменшення часу обчислення із збільшенням  $T_{\max}$  порівняно із лінійною залежністю обумовлене підвищенням ефективності паралельних обчислень із збільшенням кількості циклів.

Із табл. 3 і рис. 15 видно, що при  $L \geq 2T_{\max}$  час обчислення ВКФ від довжини ЦП не залежить, оскільки у кожному циклі обчислення ВКФ використовується ЦП довжиною  $2l$ . Із табл. 3, 4 і рис. 15 видно, що час обчислення ВКФ знаходиться у поліноміальній залежності другого ступеню від  $T_{\max}$ . Коефіцієнти полінома визначаються параметрами ЕОМ та ефективністю програмної реалізації алгоритмів і, на відміну від АКФ, не залежать від довжини ЦП.



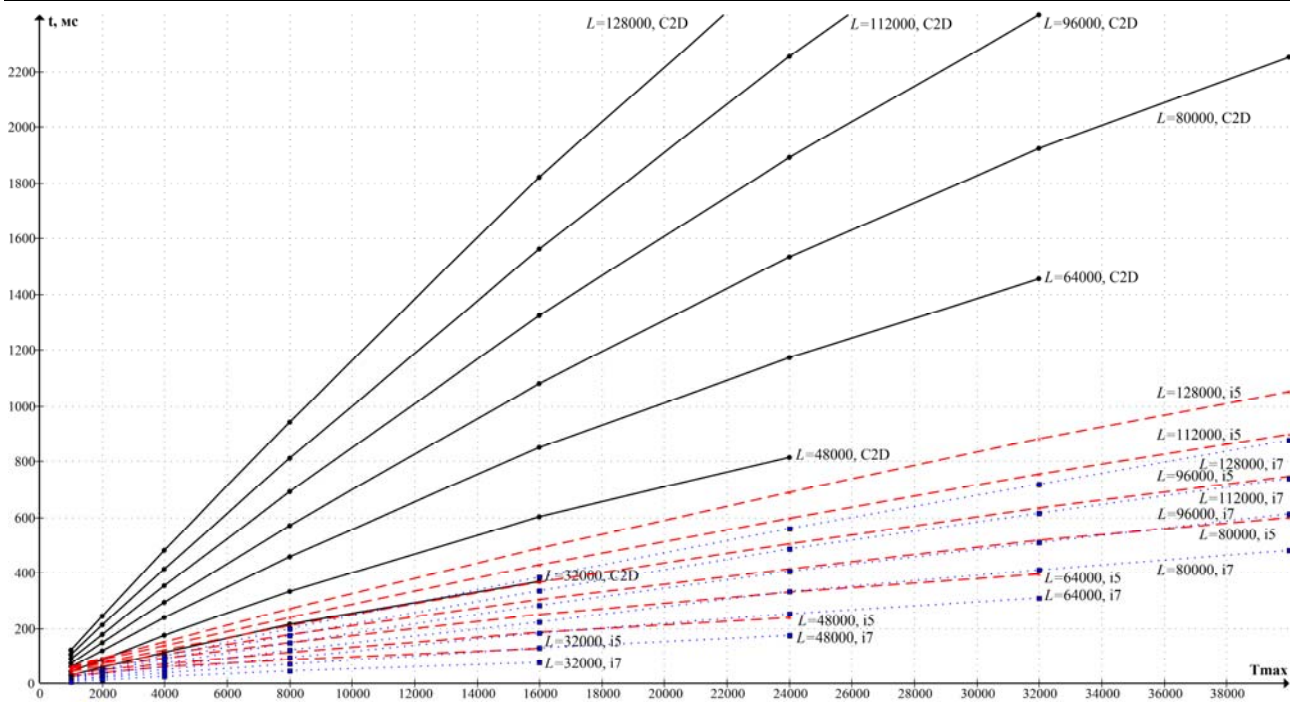


Рисунок 14 – Графік залежності часу обчислення АКФ від максимально можливого періоду  $T_{\max}$

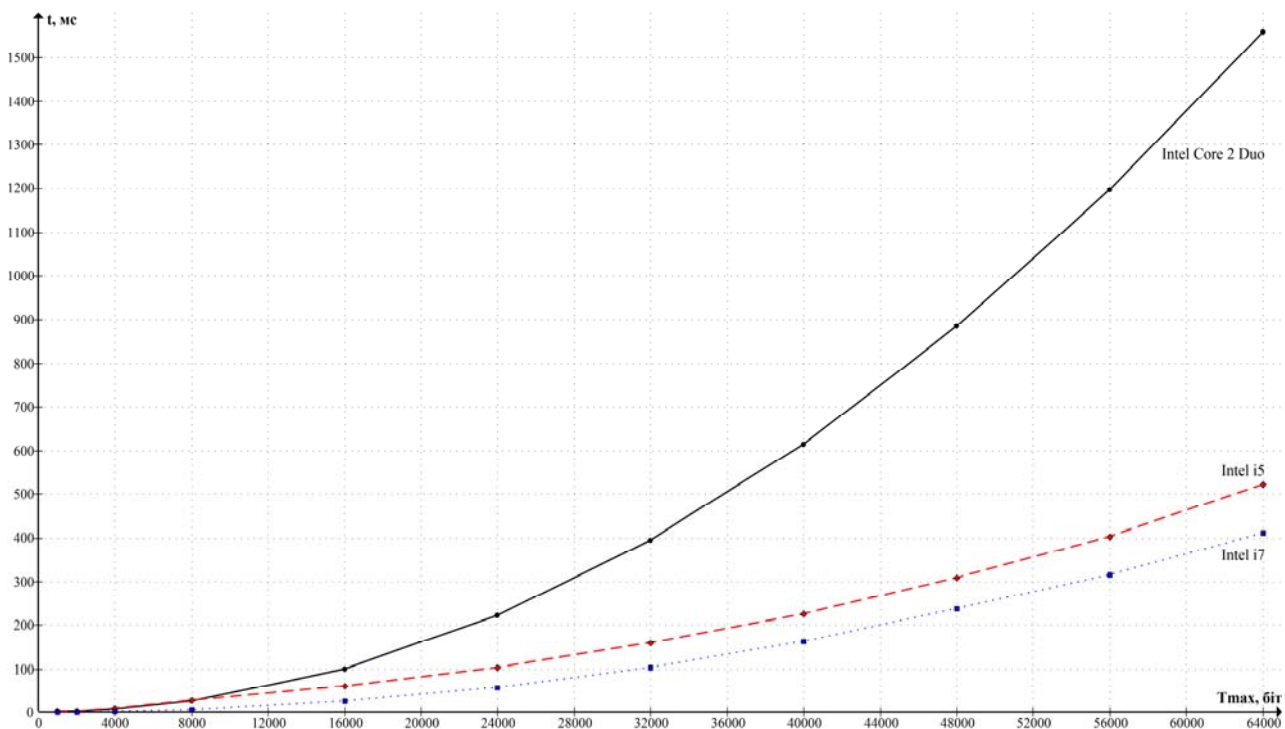


Рисунок 15 – Графік залежності часу обчислення ВКФ від максимально можливого періоду  $T_{\max}$

Час, витрачений на пошук АКФ і ВКФ, за обома алгоритмами від істинного значення періоду ЦП не залежить. Він також не залежить і від порядку заповнення ЦП, а визначається кількістю операцій у запропонованих алгоритмах для заданих  $L$  і  $T_{\max}$ .

Той факт, що для обчислень кореляційних функцій достатньо ЦП довжиною лише  $L_{\min}=2T$ , обумовлює порівняно невеликий обсяг обчислень. Період ЦП довжиною 100000 біт ( $T_{\max}$  – не більше 50000 біт) за

запропонованими алгоритмами при програмній реалізації з підтримкою паралельних обчислень на багатоядерних центральних процесорах сучасних ЕОМ може бути обчислений у масштабі реального часу: при пошуку за АКФ менше 1 с, а за ВКФ – менше 0,5 с.

В умовах апріорної невизначеності періоду  $T$  довжина ЦП  $L$  і її максимально можливий період  $T_{\max}$  можуть бути задані значно більше істинного періоду  $T$ .

## ВИСНОВКИ

В роботі вперше отримано два алгоритми пошуку періодичностей у ЦП з блоковим ЗК в умовах часткової апіорної невизначеності виду і параметрів ЗК за АКФ і ВКФ ЦП та досліджено ефективність їх застосування.

Проведений експеримент підтвердив працездатність розроблених алгоритмів щодо визначення періоду ЦП. При застосуванні обох алгоритмів отримано приблизно однакові результати кореляційних характеристик ЦП.

На відміну від відомих раніше, обидва отриманих алгоритми дозволяють здійснювати пошук періоду ЦП у масштабі реального часу навіть при великих значеннях періоду ЦП. Час обчислення ВКФ в декілька разів менше часу обчислення АКФ, тому алгоритм пошуку періоду ЦП за ВКФ її складових є ефективнішим за алгоритм пошуку періоду ЦП за АКФ.

При проведенні експериментальних досліджень основна увага зосереджена на швидкодії алгоритмів. У подальшому доцільно дослідити вплив довжини і структури СП та ймовірності помилки у ЦП на величину максимумів кореляційних функцій.

До **недоліків** обох алгоритмів слід віднести слабку здатність пошуку періодичностей у ЦП з короткими СП. Робота над усуненням цього недоліку обумовлює напрямок **подальших наукових досліджень**.

**Практичне значення** отриманих результатів полягає у можливості визначення з допомогою розроблених алгоритмів у масштабі реального часу періоду ЦП для подальшого розпізнавання на його основі виду і параметрів ЗК у ЦП.

## ЛІТЕРАТУРА / LITERATURA

1. Morelos-Zaragoza R. H. The Art of error correcting coding. 2nd ed. / Robert H. Morelos-Zaragoza. – Chichester : John Wiley & Sons, 2006. – 278 p.
2. Зубарев Ю. Б. Помехоустойчивое кодирование в цифровых системах передачи данных [Электрон. ресурс] / Ю. Б. Зубарев, Г. В. Овечкин // Электросвязь. – 2008. – № 12. – С. 58–61. – Режим доступа: [http://mtdbest.ru/articles/obzor\\_dvoichnie\\_kodi\\_2.pdf](http://mtdbest.ru/articles/obzor_dvoichnie_kodi_2.pdf).
3. TC Synchronization and Channel Coding. – Blue Book. Issue 3 [Electronic resource]. – Washington : CCSDS, 2017. – 50 p. – Access mode: <https://public.ccsds.org/Pubs/231x0b3.pdf>.
4. Сидоркина Ю. А. Анализ эффективности современных помехоустойчивых кодов [Электрон. ресурс] / Ю. А. Сидоркина, Б. И. Шахтарин, К. А. Балахонов // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». – 2014. – № 6. – С. 108–116. – Режим доступа: <https://cyberleninka.ru/article/n/analiz-effektivnosti-sovremennyh-pomeho-ustoychivyh-kodov>.
5. Котюбин В. Ю. Особенности визначення періодичності у інформаційній послідовності при проведенні технічного аналізу сигналів / В. Ю. Котюбин, О. М. Романов, Д. Ю. Бурлак // Теорія та практика створення, розвитку і застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції : XXII Всеукраїнська науково-практична конференція, Житомир, 26–27 квітня 2018 р. : тези доповідей. – Житомир : ЖВІ імені С. П. Корольова, 2018. – С. 153.
6. Романов О. М. Особенности разработки комплексов анализа цифровых последовательностей / О. М. Романов // Створення та модернізація озброєння і військової техніки в сучасних умовах : 17 науково-технічна конференція, Чернігів, 7–8 вересня 2017 р. : збірник тез доповідей. – Чернігів : ДНВЦ ЗС України, 2017. – С. 309–310.
7. Proximity-1 Space Link Protocol – Coding and Synchronization Sublayer. – Blue Book. Issue 1 [Electronic resource]. – Washington : CCSDS, 2003. – 24 p. – Access mode: <https://public.ccsds.org/Pubs/211x2b1s.pdf>.
8. Алгоритм распознавания типа и оценки параметров помехоустойчивых кодов / [С. Н. Кириллов, В. А. Ревуцкий, Д. С. Семин и др.] // Цифровая обработка сигналов и ее применение DSPA – 2011 : 13-я Международная конференция, Москва, 30 марта–1 апреля 2011 г. : доклады. – Москва : Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова, 2011. – Выпуск XIII – 2. – С. 30–33.
9. Ревуцкий В. А. Устойчивые к мешающим факторам алгоритмы распознавания вида помехоустойчивых кодов в радиотехнических системах : автореф. дис. к-та техн. наук : 05.12.04 «Радиотехника, в том числе системы и устройства телевидения» / В. А. Ревуцкий. – Рязань : РГРТУ, 2013. – 19 с.
10. Теоретические основы радиолокации. Учебное пособие для вузов / Под ред. Ширмана Я. Д. – М. : «Советское радио», 1970. – 560 с.
11. Susek W. Noise Radar with Microwave Correlation Receiver / W. Susek, B. Stec, Cz. Rećko // Acta Physica Polonica A. – 2011. – Vol. 119, № 4. – P. 483–487.
12. Advanced Ultrawideband Radar : Signals, Targets, and Applications / ed. by James D. Taylor. – Boca Raton, FL : CRC Press, Taylor & Francis Group, 2016. – 476 p.
13. Ifeakor E. C. Digital Signal Processing : a practical approach. 2nd ed. / Emmanuel C. Ifeakor, Barrie W. Jervis. – Harlow, New York : Prentice Hall, 2002. – 933 p.
14. Sklar B. Digital communications. Fundamentals and applications. 2nd ed. / Bernard Sklar. – New Jersey : Prentice Hall, 2001. – 1104 p.
15. Digital Video Broadcasting (DVB). Framing structure, channel coding and modulation for 11/12 GHz satellite services : EN 300 421 V1.1.2 (1997-08). – Sophia Antipolis : European Telecommunications Standards Institute, 1997. – 24 p.

Статья поступила в редакцию 01.06.2020.  
После доработки 01.04.2021.

УДК 621.391

## АЛГОРИТМЫ ПОИСКА ПЕРИОДИЧНОСТЕЙ В ЦИФРОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ С БЛОЧНЫМ КОДИРОВАНИЕМ ПО ИХ КОРРЕЛЯЦИОННЫМ СВОЙСТВАМ

**Романов А. Н.** – канд. техн. наук, заместитель начальника по научной работе, научно-исследовательский институт Министерства обороны Украины, Киев, Украина.

© Романов О. М., Котюбин В. Ю., 2021  
DOI 10.15588/1607-3274-2021-2-1

**Котюбин В. Ю.** – научный сотрудник, научно-исследовательский институт Министерства обороны Украины, Киев, Украина.

### АННОТАЦИЯ

**Актуальность.** Для повышения помехоустойчивости систем связи и передачи данных широко применяется помехоустойчивое кодирование. Наиболее распространенными в силу своей эффективности являются методы блочного кодирования. В условиях частичной априорной неопределенности вида и параметров кодирования перед декодированием цифровой последовательности проводится предварительный анализ для их определения. При блочном кодировании для определения периода цифровой последовательности, обусловленного добавлением к ней синхропоследовательности, и который может определять вид и параметры кодирования, распространенным подходом является использование их корреляционных свойств.

**Целью** работы является изложение алгоритмов поиска периодичностей в цифровых последовательностях с блочным помехоустойчивым кодированием в условиях частичной априорной неопределенности вида и параметров помехоустойчивого кода.

**Метод.** В статье приведены два алгоритма поиска периодичностей в цифровых последовательностях с блочным кодированием и описан принцип их работы. В основе одного алгоритма лежит вычисление АКФ, в основе другого – ВКФ. Показано, что длина цифровой последовательности должна быть в два раза больше максимально возможного периода. Работа обоих алгоритмов проиллюстрирована примерами.

**Результаты.** На основе предложенных алгоритмов разработано специальное программное обеспечение. Результаты определения периода цифровых последовательностей с блочным помехоустойчивым кодированием при различных значениях периода подтвердили работоспособность предложенных алгоритмов. Оба предложенных алгоритма дают примерно одинаковый результат. Установлены экспериментальные зависимости времени вычисления АКФ и ВКФ от длины цифровой последовательности и максимально возможного периода. Алгоритм поиска периода цифровой последовательности с помощью ВКФ ее составляющих является более эффективным из-за меньшего количества вычислений.

**Выводы.** В работе впервые получены два алгоритма поиска периодичностей в цифровых последовательностях с блочным помехоустойчивым кодированием, основанные на определении их корреляционных функций. Применение разработанных алгоритмов на практике позволяет в условиях частичной априорной неопределенности вида и параметров помехоустойчивого кода определять период цифровых последовательностей в масштабе реального времени даже при больших значениях периода, а на его основе – идентифицировать вид и параметры блочных помехоустойчивых кодов.

**КЛЮЧЕВЫЕ СЛОВА:** автокорреляционная функция, взаимная корреляционная функция, цифровая последовательность, период, блочный помехоустойчивый код, синхропоследовательность, система связи и передачи данных.

UDC 621.391

### PERIODICITY SEARCH ALGORITHMS IN DIGITAL SEQUENCES WITH BLOCK CODING BY THEIR CORRELATION PROPERTIES

**Romanov O. M.** – PhD, Deputy Head for Research, Research Institute of the Ministry of Defense of Ukraine, Kiev, Ukraine.  
**Kotiubin V. Yu.** – Researcher, Research Institute of the Ministry of Defense of Ukraine, Kiev, Ukraine.

### ABSTRACT

**Context.** To improve the noise immunity of communication and data transmission systems, error-correcting coding is widely used. The most common because of their effectiveness are block coding methods. Under conditions of partial a priori uncertainty of the type and parameters of encoding, before decoding the digital sequence, a preliminary analysis is carried out to determine them. In block coding, to determine the period of a digital sequence caused by the addition of a sync sequence to it, and which can determine the type and parameters of coding, a common approach is to use their correlation properties.

**Objective.** The object of the research is the presentation of periodicity search algorithms in digital sequences with block error-correcting coding under conditions of partial a priori uncertainty of the type and parameters of the error-correcting code.

**Method.** The article presents two periodicity search algorithms in digital sequences with block coding and describes the principle of their operation. The basis of one algorithm is the calculation of the autocorrelation function, the basis of the other is calculation of the cross-correlation function. It is shown that the length of the digital sequence should be twice as long as the maximum possible period. The operation of both algorithms is illustrated by examples.

**Results.** Based on the proposed algorithms, special software has been developed. The results of determining the period of digital sequences with block error-correcting coding at different values of the period confirmed the efficiency of the proposed algorithms. Both proposed algorithms give approximately the same result. Experimental dependences of the calculation time of auto- and cross-correlation functions from the length of the digital sequence and the maximum possible period are established. The period search algorithm in a digital sequence, that use the cross-correlation function of its components, is more efficient due to fewer calculations.

**Conclusions.** For the first time, two periodicity search algorithms in digital sequences with block error-correcting based on the determination of their correlation functions are obtained. The application of the developed algorithms in practice allows, under partial a priori uncertainty of the type and parameters of the error-correcting code, to determine the period of digital sequences in real time even at large values of the period, and based on it, to identify the type and parameters of block error-correcting codes.

**KEYWORDS:** autocorrelation function, cross-correlation function, digital sequence, period, block error-correcting code, synchronization sequence, communication and data transmission system.

## REFERENCES

1. Morelos-Zaragoza R. H. The Art of error correcting coding. 2nd ed. Chichester : John Wiley & Sons, 2006, 278 p.
2. Zubarev Ju. B., Ovechkin G. V. Pomehoustojchivoe kodirovanie v cifrovyyh sistemah peredachi dannyh [Electronic resource], *Jelektrosvjaz'*, 2008, No. 12, pp. 58–61. Access mode: [http://mtdbest.ru/articles/obzor\\_dvoichnie\\_kodi\\_2.pdf](http://mtdbest.ru/articles/obzor_dvoichnie_kodi_2.pdf).
3. TC Synchronization and Channel Coding. Blue Book. Issue 3 [Electronic resource]. Washington, CCSDS, 2017, 50 p. Access mode: <https://public.ccsds.org/Pubs/231x0b3.pdf>.
4. Sidorkina Ju. A., Shahtarin B. I., Balahonov K. A. Analiz jeffektivnosti sovremennyh pomehoustojchivyh kodov [Electronic resource], *Vestnik MGTU im. N. Je. Baumana. Ser. "Priborostroenie"*, 2014, No. 6, pp. 108–116. Access mode: <https://cyberleninka.ru/article/n/analiz-effektivnosti-sovremennyh-pomehoustojchivyh-kodov>.
5. Kotjubin V. Ju., Romanov O. M., Burlak D. Ju. Osoblyvosti vyznachennja periodychnosti u informacijnij poslidovnosti pry provedeni tehničnogo analizu sygnaliv. *Teorija ta praktyka stvorennja, rozvytku i zastosuvannja vysokotehnologichnyh system special'nogo pryznachennja z urahuvannjam dosvidu antyterrorystychnoi' operacii' : XXII Vseukrai'ns'ka naukovo-praktyčna konfere-ncija, Zhytomyr, 26–27 kvitnja 2018 r. : tezy dopovidej*. Zhytomyr ZhVI imeni S. P. Korol'ova, 2018, P. 153.
6. Romanov O. M. Osoblyvosti rozrobky kompleksiv analizu cyfrovyyh poslidovnostej, *Stvorennja ta modernizacija ozbrojennja i vijs'kovoï' tehniky v suchasnyh umovah : 17 naukovo-tehnična konferencija, Chernigiv, 7–8 veresnja 2017 r. : zbirnyk tez dopovidej*. Chernigiv, DNVC ZS Ukrai'ny, 2017, pp. 309–310.
7. Proximity-1 Space Link Protocol – Coding and Synchronization Sublayer. Blue Book. Issue 1 [Electronic resource]. Washington, CCSDS, 2003, 24 p. Access mode: <https://public.ccsds.org/Pubs/211x2b1s.pdf>.
8. Kirillov S. N., Revuckij V. A., Semin D. S. i dr. Algoritm raspoznavanija tipa i ocenki parametrov pomehoustojchivyh kodov, *Cifrovaja obrabotka signalov i ee primenenie DSPA – 2011 : 13-ja Mezhdunarodnaja konferencija, Moskva, 30 marta–1 aprlja 2011 g. : doklady*. Moscow : Rossijskoe nauchno-tehničeskoe obshhestvo radiotekhniki, jelektroniki i svjazi im. A. S. Popova, 2011, Vypusk XIII – 2, pp. 30–33.
9. Revuckij V. A. Ustojchivye k meshajushhim fakto-ram algoritmy raspoznavanija vida pomeho-ustojchivyh kodov v radiotekhnicheskijh sistemah : avtoref. dis. ... k-ta tehn. nauk : 05.12.04 "Radiotekhnika, v tom chisle sistemy i ustrojstva televidenija". Rjazan', RGRTU, 2013, 19 p.
10. Teoreticheskie osnovy radiolokacii. Uchebnoe posobie dlja vuzov / Pod red. Shirmana Ja. D. Moscow, "Sovetskoe radio", 1970, 560 p.
11. Susek W., Stec B., Rečko Cz. Noise Radar with Microwave Correlation Receiver, *Acta Physica Polonica A*, 2011, Vol. 119, No. 4, pp. 483–487.
12. Advanced Ultrawideband Radar : Signals, Targets, and Applications, ed. by James D. Taylor. Boca Raton, FL, CRC Press, Taylor & Francis Group, 2016, 476 p.
13. Ifeachor E. C., Jervis B. W. Digital Signal Processing : a practical approach. 2nd ed. Harlow. New York, Prentice Hall, 2002, 933 p.
14. Sklar B. Digital communications. Fundamentals and applications. 2nd ed. New Jersey, Prentice Hall, 2001, 1104 p.
15. Digital Video Broadcasting (DVB). Framing structure, channel coding and modulation for 11/12 GHz satellite services : EN 300 421 V1.1.2 (1997-08). Sophia Antipolis, European Telecommunications Standards Institute, 1997, 24 p.