Використано поліноміальний підхід до розв'язку задачі спільного розрізнення радіосигналів та оцінювання їх параметрів на фоні негаусівських завад. Адаптовано метод максимізації усіченого стохастичного полінома та моментний критерій якості для розв'язування багатоальтернативних задач перевірки статистичних гіпотез. Представлено результати комп'ютерного моделювання синтезованих алгоритмів з використанням генератора псевдовипадкових послідовностей, що базуються на бігаусовій моделі

Ключові слова: усічені стохастичні поліноми, моментні критерії якості, розрізнення сигналів, негаусівські завади

Использован полиномиальный подход к решению задачи совместного различения радиосигналов и оценивания их параметров на фоне аддитивной асимметричной помехи. Адаптирован метод максимизации усеченного стохастического полинома и моментный критерий качества для решения многоальтернативных задач проверки статистических гипотез. Представлены результаты компьютерного моделирования синтезированных алгоритмов с использованием генератора псевдослучайных последовательностей, основанных на бигауссовой модели

Ключевые слова: усеченные стохастические полиномы, моментные критерии качества, различение сигналов, негауссовские помехи

УДК 621.37:621.391
DOI: 10.15587/1729-4061.2014.28006

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ПОЛІНОМІАЛЬНИХ АЛГОРИТМІВ РОЗРІЗНЕННЯ РАДІОСИГНАЛІВ ТА ОЦІНЮВАННЯ ЇХ ПАРАМЕТРІВ

В. В. Палагін
Доктор технічних наук, професор*
E-mail: palahin@yahoo.com
А. В. Гончаров
Кандидат технічних наук, доцент*
E-mail: artyom28@gmail.com
В. М. Уманець
Аспірант*
E-mail: vladimirumanets@gmail.com
*Кафедра радіотехніки
Черкаський державний технологічний університет
бул. Шевченка, 460, м. Черкаси, Україна, 18006

1. Вступ

При розгляді загальної теорії статистичної обробки сигналів виділяються два самостійні напрями [1, 2], які добре вивчені і знайшли своє широке застосування для рішення багатьох практичних задач. Перший напрям стосується питань перевірки статистичних гіпотез і використовується для вирішення таких прикладних завдань, як виявлення сигналів, розрізнення і розпізнавання на фоні завад, де рішення виноситься з певної дискретної множини. Другий напрям стосується оцінювання параметрів сигналів на фоні завад, які, як правило, є безперервними величинами. З іншого боку існує велика кількість задач, де необхідно суміщати ці два напрями теорії статистичної обробки сигналів, що призводить до побудови двофункціональних правил [1] вибору рішень при спільному розрізненні сигналів та оцінюванні їх параметрів.

Традиційно для побудови двофункціональних правил використовують добре відомі класичні методи теорії статистичної обробки сигналів [1], які в загальному виє падку не передбачають обмежень на використання виду щільності розподілу випадкових величин. На практиці значного поширення набуло застосування стандартного нормального розподілу випадкових величин, яке в багатьох випадках унеможливлює відображення реальних процесів з необхідною адекватністю.

Використання традиційного підходу до дослідження і розробки систем обробки випадкових негаусівських процесів характеризується суттєвими обмеженнями, пов'язаними зі складністю їх алгоритмічної реалізації, зростанням обчислювальних ресурсів, що призводить до відповідних труднощів при створенні якісних програмно-алгоритмічних та апаратних засобів обробки сигналів.

В зв'язку з цим актуальною постає задача побудови ефективних методів обробки сигналів, що дозволяють підвищити точність обробки негаусівських сигналів порівняно з традиційним кореляційним підходом при заданих обмеженнях на їх алгоритмічну та обчислювальну складність.

2. Аналіз літературних даних

Узагальнені методи, які застосовуються для побудови двофункціональних правил (Баєсівський метод, метод максимальної правдоподібності та ін.), не обмежують клас випадкових величин, разом з тим на практиці широке застосування знайшли гаусівські моделі випадкових сигналів, що пояснюється зручністю використання математичного апарату.

Кожен з методів, що базується на використанні гаусівської моделі випадкових сигналів, має свої пе-

реваги та недоліки. Реалізація Баєсівського методу [3] передбачає знання щільності розподілу випадкової величини, що стає його основною проблемою. Застосування методу максимальної правдоподібності [4] не підходить для практичної реалізації в більшості систем через високу обчислювальну складність. Труднощі розрахунку пов'язані з необхідністю знати закон розподілу випадкової величини, що не завжди виявляється можливим. В таких випадках часто використовується метод моментів [5], що не володіє властивостями асимптотичної оптимальності, але часто приводить до порівняно простих розрахунків.

Розглянуті методи на основі гаусівської моделі не враховують більш складну структуру реальних завад, внаслідок чого точність алгоритмів обробки сигналів може буде недостатньою [6, 7]. В зв'язку з цим актуальною являється задача розробки нових алгоритмів з використанням негаусівських моделей сигналів та завад.

Результати досліджень останніх років [8] свідчать про те, що при вирішенні задач обробки негаусівських процесів перспективним є підхід, в якому для опису статистичних властивостей випадкових величин використовуються моменти і кумулянти, що дозволяє з прийнятним наближенням характеризувати статистичні властивості негаусівських процесів [6, 7]. Зокрема, кумулянти і кумулянтні коефіцієнти, на відміну від моментів, мають самостійний статистичний сенс і дають можливість описувати ступінь негаусівських розподілів випадкових величин. Такий підхід дозволяє підвищити точність обробки негаусівських сигналів у порівнянні з традиційним підходом.

В даній роботі будемо використовувати нові двофункціональні правила вибору рішень на основі моментно-кумулянтного опису випадкових величин, моментний критерій якості верхніх границь ймовірностей помилок для багатоальтернативної перевірки статистичних гіпотез та метод максимізації усіченого стохастичного полінома.

Запропонований підхід дозволяє будувати двофункціональні правила обробки сигналів на основі застосування моментно-кумулянтного опису випадкових величин, що дає можливість, з одного боку, спростити спільні алгоритми розрізнення сигналів і оцінювання їх параметрів, а з іншого боку, – збільшити їхню ефективність у вигляді зменшення ймовірностей помилок РП та зменшення дисперсій оцінок за допомогою врахування характеристик негаусівських завад.

3. Мета та задачі дослідження

Нехай на вході системи спостерігається випадковий сигнал, який представляє собою адитивну суміш корисного сигналу $S_i(t)$ та завади $\eta(t)$: $\xi_i(t) = S_i(t) + \eta(t)$. Обробці підлягають вибіркові значення $\mathbf{X} = (x_1, x_2, .., x_n)$ обсягу n з послідовності незалежних і неоднаково розподілених випадкових величин. За результатами обробки $\mathbf{X}$ необхідно винести рішення про реалізацію однієї з гіпотез H_i, $i = \overline{0,N}$. Замінивши безперервний час спостереження t на дискретні відліки v обсягом n для досліджуваного сигналу $\xi_i(t)$ в припущенні стаціонарності негаусівських завад можемо записати:

$$H_i: \xi_{iv} = S_{iv}(\alpha_k) + \eta(\gamma_k),\ i = \overline{1,N},\ v = \overline{1,n};$$

$$H_0: \xi_{0v} = \eta(\gamma_k),$$

де S_{iv} – значення і -го радіосигналу з відомими (оціночними) параметрами у вигляді моментно-кумулянтного опису α_k в v -й момент часу; $\eta(\gamma_k)$ – негаусівська випадкова величина з відомими (оціночними) параметрами у вигляді моментно-кумулянтного опису γ_k. За результатами обробки $\mathbf{X}$ необхідно винести рішення про реалізацію однієї з гіпотез H_i, $i = \overline{0,N}$.

Запропоновані моделі можуть бути застосовані до різного класу сигналів і завад. Однак для отримання конкретних результатів та ілюстрації ефективності поліноміальних методів розрізнення сигналів та оцінювання їх параметрів на фоні негаусівських завад пропонується розглянути суміш радіосигналу і асиметрично-ексцесної негаусівської завади. В якості корисного сигналу обрано радіосигнал в силу його широкого застосування в багатьох додатках. Асиметрично-ексцесна завада другого типу першого виду характеризується відмінними від нуля коефіцієнтами асиметрії γ_3 та ексцесу γ_4 (всі інші кумулянтні коефіцієнти вищого порядку дорівнюють нулю) і має місце в різних каналах зв'язку.

Метою роботи є створення та реалізація моделей процесів спільного розрізнення радіосигналів та оцінювання їх параметрів на фоні негаусівських завад. На основі моментно-кумулянтного представлення випадкових величин необхідно сформувати моментні критерії якості перевірки статистичних гіпотез, поліноміальні розв'язувальні правила (РП) та поліноміальні алгоритми спільного оцінювання параметрів випадкових величин.

Задачі дослідження: побудова ефективних методів і комп'ютерних засобів функціонування систем прийому та обробки даних відповідного класу, які б дозволили підвищити точність результатів обробки сигналів.

4. Синтез структурної схеми системи спільного розрізнення сигналів та оцінювання їх параметрів

В роботі пропонується використати двофункціональне правило обробки вхідних вибіркових значень $\mathbf{X}$:

$$\Delta[\mathbf{X}] = F\{\Delta_p[\mathbf{X}], \Delta_o[\mathbf{X}]\},$$

де $\Delta_p[\mathbf{X}]$ – функція розрізнення гіпотез, в основу якої покладено застосування поліноміальних РП розрізнення сигналів, оптимальні коефіцієнти яких знаходяться згідно моментного критерію якості верхніх границь ймовірностей помилок [9], $\Delta_o[\mathbf{X}]$ – функція оцінювання параметрів сигналів, в основі якої лежать методи максимізації полінома (ММП) [6] та максимізації усіченого стохастичного полінома (ММУСП) [10].

Реалізація двофункціонального правила представлена на рис. 1. В систему надходять вибіркові значення $\mathbf{X}$ обсягом n, на основі яких необхідно прийняти рішення про реалізацію гіпотези H_i та виконати спільне оцінювання параметрів сигналу при використанні ММП і ММУСП.

Нехай прийняті сигнали містять адитивну суміш корисного сигналу $S_i(t)$ та негаусівської завади $\eta(\gamma_1, \gamma_2, \gamma_3, \gamma_4, ..., \gamma_\mu)$, що описується кінцевою послідов-

ністю кумулянтів γ_i, $i=\overline{1,\mu}$. Для зручності будемо вважати, що негаусівська завада має нульове математичне сподівання ($\gamma_1=0$), дисперсію $\gamma_2=\chi_2$ та описується коефіцієнтами третього та четвертого порядку, не рівними нулю.

Отримані в блоці 2 оцінки параметрів $\hat{\vartheta}_i$, $i=\overline{0,r}$ є псевдооцінками на множині Θ. Їх вибір відбувається в блоці 4 на основі рішення про реалізацію гіпотези H_i на користь прийняття сигналу $S_i(t)$ в блоці 3 при виборі максимального значення РП, що представлені у вигляді стохастичних поліномів $\Lambda_1\left(\mathbf{X},\hat{\vartheta}_1,\lambda_1\right)$ (блок 1), оптимальних по моментному критерію якості верхніх границь ймовірностей помилок.

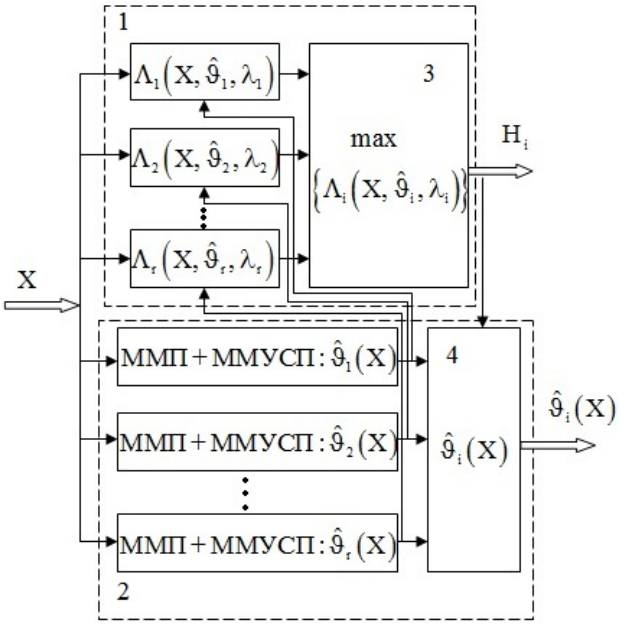


Рис. 1. Структурна схема системи спільного розрізнення сигналів і оцінювання їх параметрів: 1 – блок, що реалізує функції розрізнення сигналів $\Delta_p[\mathbf{X}]$; 2 – блок, що реалізує функції оцінювання параметрів $\Delta_o[\mathbf{X}]$; 3 – блок вибору максимального значення РП; 4 – блок оцінювання параметрів $\hat{\vartheta}_i$, $i=0,r$

На практиці немає необхідності розглядати весь широкий спектр негаусівських випадкових величин, класифікація яких представлена в [6]. Часто можна обмежитися випадковими величинами, представленими в класі асиметричних, ексцесних та асиметрично-ексцесних випадкових величин, які описуються кумулянтними коефіцієнтами третього та четвертого порядків.

5. Побудова поліноміальних алгоритмів спільного оцінювання параметрів сигналів та завад

Розглянемо спільне оцінювання параметрів радіосигналів та асиметрично-ексцесної негаусівської завади в блоці 2 (рис. 1). Припустимо для спрощення, що фаза радіосигналу дорівнює нулю, а коефіцієнти асиметрії та ексцесу негаусівської завади відомі. Тоді параметри, що оцінюються, можна представити у вигляді вектора $\vec{\vartheta}=\left(a_{0(r)},\omega_{0(r)},\chi_2\right)$, $r=\overline{1,d}$, де d – кількість радіосигналів, що досліджується. Оцінки параметрів радіосигналів знаходяться за допомогою ММП [6], а параметр завади за допомогою ММУСП [10]. Методи, що використовуються, базуються на використанні негаусівських моделей завад.

Згідно ММП та ММУСП оцінки параметрів сигналів та завади знаходяться із системи рівнянь:

$$\begin{cases}\sum\limits_{i=1}^{s}\sum\limits_{v=1}^{n}h_{i(s)1v(r)}(\vartheta)\sum\limits_{v=1}^{n}\left[x^i_{v(r)}-m_{iv(r)}(\vartheta)\right]\Big|_{\substack{a_{0(r)}=\hat{a}_{0(r)}\\ \omega_{0(r)}=\hat{\omega}_{0(r)}\\ \chi_2=\hat{\chi}_2}}=0,\\ \sum\limits_{i=1}^{s}\sum\limits_{v=1}^{n}h_{i(s)2v(r)}(\vartheta)\sum\limits_{v=1}^{n}\left[x^i_{v(r)}-m_{iv(r)}(\vartheta)\right]\Big|_{\substack{\omega_{0(r)}=\hat{\omega}_{0(r)}\\ a_{0(r)}=\hat{a}_{0(r)}\\ \chi_2=\hat{\chi}_2}}=0,\\ \sum\limits_{\substack{i=1\\ i\neq(c,e,...,l)}}^{s}\sum\limits_{v=1}^{n}h_{i(s)[3]v(r)}(\vartheta)\left[x^i_{v(r)}-m_{iv(r)}(\vartheta)\right]\Big|_{\substack{\chi_2=\hat{\chi}_2\\ a_{0(r)}=\hat{a}_{0(r)}\\ \omega_{0(r)}=\hat{\omega}_{0(r)}}}=0,\end{cases}\qquad(1)$$

де $m_{iv(r)}(\vec{\vartheta})$ – початкові моменти випадкової величини ξ, які в загальному випадку знаходяться з виразу $m_{iv(r)}(\vec{\vartheta})=E\left(S_{v(r)}+\eta\right)^i$, де $i=\overline{1,2s}$, а $\eta^i=\alpha_i$ – початкові моменти асиметрично-ексцесної завади другого типу першого виду, $x_{v(r)}$ – незалежні неоднаково розподілені вибіркові значення досліджуваної випадкової величини, $v=\overline{1,n}$ – порядковий номер вибіркового значення, n – обсяг вибірки, s – ступінь стохастичного полінома. $h_{i(s)1v(r)}(\vartheta)$, $h_{i(s)2v(r)}(\vartheta)$ – оптимальні коефіцієнти, що забезпечують мінімальні дисперсії оцінок амплітуди та частоти радіосигналів та знаходяться з системи лінійних алгебраїчних рівнянь:

$$\sum_{j=1}^{s}h_{j(s)1v(r)}(\vartheta)K_{(i,j)v(r)}(\vartheta)=\frac{\partial}{\partial a_{0(r)}}m_{iv(r)}(\vartheta),$$

$$\sum_{j=1}^{s}h_{j(s)2v(r)}(\vartheta)K_{(i,j)v(r)}(\vartheta)=\frac{\partial}{\partial \omega_{0(r)}}m_{iv(r)}(\vartheta),\ \text{де } i=\overline{1,s},$$

а коефіцієнти $h_{i(s)[3]v(r)}(\vartheta)$, знаходяться з умови мінімального значення дисперсій оцінок кумулянта другого порядку та знаходяться з системи усічених алгебраїчних рівнянь:

$$\sum_{j=1}^{s}h_{j(s)[3]v(r)}(\vartheta)K_{(i,j)v(r)}(\vartheta)=\frac{\partial}{\partial \chi_2}m_{iv(r)}(\vartheta),\ i=\overline{1,s};$$

$$i,j\neq(c,e,...,l),$$

де $K_{(i,j)v(r)}(\vartheta)=m_{(i+j)v(r)}(\vartheta)-m_{iv(r)}(\vartheta)m_{jv(r)}(\vartheta)$.

Для знаходження оцінок параметрів завади немає потреби знати всі оптимальні коефіцієнти, в нашому випадку для оцінювання параметра χ_2 беремо до уваги лише перших два оптимальних коефіцієнта. Всі інші оптимальні коефіцієнти прирівнюються до нуля, що буде достатнім для отримання необхідної мінімальної інформації про параметри завади. Підставивши вирази отриманих оптимальних коефіцієнтів, початкових моментів та вираз досліджуваного сигналу в систему рівнянь (1), отримаємо рівняння для знаходження спільних оцінок зазначених параметрів.

Для дослідження статистичних властивостей оцінок параметрів радіосигналів при різних степенях полінома s розраховуються асимптотичні дисперсії оцінок, які знаходяться з матриці кількості добутої інформації:

$$J_{sn(r)}(\vartheta)=\left\|J^{(m,k)}_{sn(r)}(\vartheta)\right\|.$$

Елементи матриці відповідно дорівнюють:

$$J^{(m,k)}_{sn(r)}(\vartheta)=\sum_{v=1}^{n}\sum_{i=1}^{s}\sum_{j=1}^{s}h_{i(s)mv(r)}(\vartheta)h_{j(s)kv(r)}(\vartheta)K_{(i,j)v(r)}(\vartheta),$$

$m,k=\overline{1,3}$.

Дисперсії оцінок параметрів сигналу дорівнюють відповідним діагональним елементам варіаційної матриці, яка асимптотично при $(n\to\infty)$ дорівнює оберненій матриці кількості добутої інформації.

Ефективність запропонованих методів досліджується за допомогою коефіцієнтів зменшення дисперсій отриманих оцінок (рис. 2), які знаходяться з виразу:

$$g_{sk}=\frac{\sigma^2_s}{\sigma^2_k}.$$

При $(n\to\infty)$ буде справедлива рівність:

$$g_{\left(a_{0(r)}\right)^{sk}}=g_{\left(\omega_{0(r)}\right)^{sk}}=\frac{\sigma^2_{\left(a_{0(r)}\right)^s}}{\sigma^2_{\left(a_{0(r)}\right)^k}}=\frac{\sigma^2_{\left(\omega_{0(r)}\right)^s}}{\sigma^2_{\left(\omega_{0(r)}\right)^k}}.$$

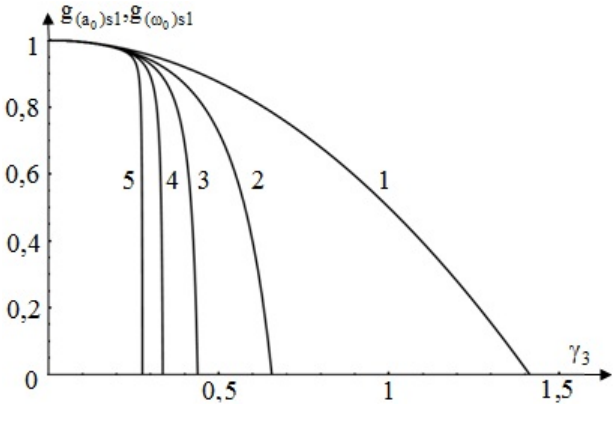
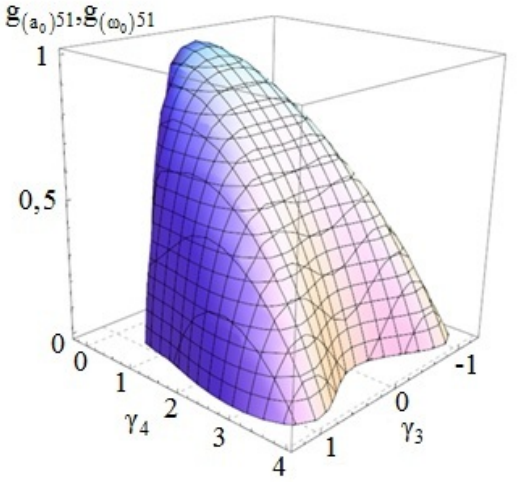


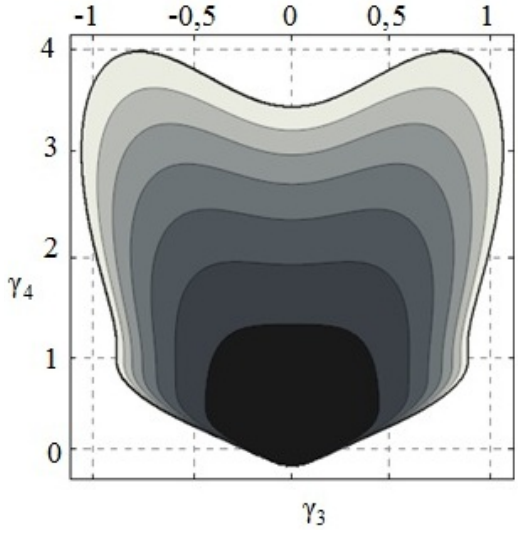
Рис. 2. Залежність коефіцієнтів зменшення дисперсій оцінок $g_{(a_0)s1},g_{(\omega_0)s1}$ від коефіцієнта асиметрії γ_3, коефіцієнт ексцесу $\gamma_4=0$: 1 – $g_{(a_0)31},g_{(\omega_0)31}$, 2 – $g_{(a_0)41},g_{(\omega_0)41}$, 3 – $g_{(a_0)51},g_{(\omega_0)51}$, 4 – $g_{(a_0)61},g_{(\omega_0)61}$

На рис. 3, *а* представлено залежність дисперсій оцінок у вигляді об'ємного графіку, а на рис. 3, *б* – у вигляді проекції лінії рівнів на площину.

З побудованих графіків функцій коефіцієнтів зменшення дисперсій отриманих оцінок (рис. 2, 3) видно, що зі зростанням степеня стохастичного полінома та по мірі наближення коефіцієнтів асиметрії та ексцесу до границі області допустимих значень, ефективність поліноміальних методів оцінювання параметрів, які базуються на використанні негаусівських моделей завад, збільшується.



а



б

Рис. 3. Залежність коефіцієнтів зменшення дисперсій оцінок $g_{(a_0)51},g_{(\omega_0)51}$ від коефіцієнтів γ_3 та γ_4: *а* – загальний вигляд об'ємного графіка; *б* – проекція ліній рівнів на площину

6. Побудова методів розрізнення радіосигналів при використанні моментного критерію якості верхніх границь ймовірностей помилок

Розглянемо окремий випадок перевірки трьох статистичних гіпотез, що реалізується в блоці 1 (рис. 1):

H_0 – прийнята завада: $\xi_{0v}=\eta(\gamma_k)$; H_1 – прийнятий сигнал S_{1v}: $\xi_{1v}=S_{1v}(\alpha_k)+\eta(\gamma_k)$; H_2 – прийнятий сигнал S_{2v}: $\xi_{2v}=S_{2v}(\alpha_k)+\eta(\gamma_k)$, де S_{1v} та S_{2v} – інформативні радіосигнали, що приймають наступний загальний вигляд:

$$S_{iv}=a_{0i}\,r_{iv}\cos(\omega_{0i}v\,\delta),$$

де a_{0i} – амплітуда радіосигналу, r_{iv} – обвідна радіосигналу, ω_{0i} – частота, $i=1,2$, δ – крок дискретизації.

Для неоднаково розподілених вибіркових значень і використання моментного критерію якості [9] необхідно використати стохастичний поліном для розрізнення гіпотез H_m і H_r наступного вигляду:

$$\Lambda(\mathbf{X})^{(mr)}_{sn}=\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}x_v^i+k_0^{(mr)}\underset{H_r}{\overset{H_m}{\gtrless}}0\ ,$$

$$r,m=\overline{0,\,N-1},\ r\neq m\ , \qquad (2)$$

де $k_0^{(mr)}=-\frac{1}{2}\left(E_m^{(mr)}+E_r^{(mr)}\right)=-\frac{1}{2}\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}\left(m_{iv}^{(m)}+m_{iv}^{(r)}\right)$. (3)

Невідомі оптимальні коефіцієнти $k_{iv}^{(mr)}$ РП (2), які мінімізують обраний критерій якості, знаходяться із розв'язку системи лінійних алгебраїчних рівнянь:

$$\sum_{j=1}^{s}k_{jv}^{(mr)}\left[F_{(i,j)v}^{(r)}+F_{(i,j)v}^{(m)}\right]=m_{iv}^{(m)}-m_{iv}^{(r)},\ v=\overline{1,n},\ i=\overline{1,s}\ . \qquad (4)$$

Математичні сподівання й дисперсії РП (2) приймуть вигляд:

$$E_m^{(mr)}=\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}m_{iv}^{(m)},\ E_r^{(mr)}=\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}m_{iv}^{(r)}\ ,$$

$$G_m^{(mr)}=\sum_{i=s}^{s}\sum_{j=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}k_{jv}^{(mr)}F_{(i,j)v}^{(m)}\ ,$$

$$G_r^{(mr)}=\sum_{i=s}^{s}\sum_{j=1}^{s}\sum_{v=1}^{n}k_{iv}^{(mr)}k_{jv}^{(mr)}F_{(i,j)v}^{(r)}\ ,$$

де $m_{iv}^{(r)}$, $m_{iv}^{(m)}$ – початкові моменти i-го порядку випадкової величини ξ при гіпотезах $H^{(m)}$ і $H^{(r)}$ для v-го значення відповідно, $F_{(i,j)v}^{(r)}$, $F_{(i,j)v}^{(m)}$ – центровані корелянти випадкової величини (i,j)-го порядку при гіпотезах $H^{(m)}$ і $H^{(r)}$ відповідно для v-го значення та записуються у вигляді:

$$F_{(i,j)v}^{(m)}=m_{(i+j)v}^{(m)}+m_{iv}^{(m)}m_{jv}^{(m)},\ F_{(i,j)v}^{(r)}=m_{(i+j)v}^{(r)}+m_{iv}^{(r)}m_{jv}^{(r)}\ .$$

Тоді загальна структура РП для вибору гіпотези $H^{(m)}$ прийме вигляд:

$$H_m:\ \max_{m=\overline{1,N-1}}\left\{\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(m0)}x_v^i+k_0^{(m0)}\right\}>0;$$

$$H_0:\max_{m=\overline{1,N-1}}\left\{\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(m0)}x_v^i+k_0^{(m0)}\right\}<0.$$

$$\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(m0)}x_v^i+k_0^{(m0)}>\sum_{i=1}^{s}\sum_{v=1}^{n}k_{iv}^{(r0)}x_v^i+k_0^{(r0)},$$

$$r,m=\overline{1,\,N-1},\ r\neq m\ .$$

Кількість добутої інформації з вибіркових значень про розрізнення гіпотез запишеться у вигляді:

$$I_{Ku\,sn}^{(mr)}=\sum_{v=1}^{n}\sum_{i=1}^{s}k_{jv}^{(mr)}k_{iv}^{(mr)}\left[F_{(i,j)v}^{(m)}+F_{(i,j)v}^{(r)}\right]=$$

$$=\sum_{v=1}^{n}\sum_{i=1}^{s}k_{iv}^{(mr)}\left(m_{iv}^{(m)}-m_{iv}^{(r)}\right), \qquad (5)$$

$$m,r=\overline{0,N-1},m\neq r\ .$$

Для якісної оцінки отриманих РП розрізнення сигналів на фоні завад введемо величину, що характеризує загальні верхні границі ймовірностей помилок розрізнення гіпотези $H^{(m)}$ при обробці N РП:

$$Ku(E,G)^{(m)}=\sum_{r=0}^{N-1}\frac{G_m^{(mr)}+G_r^{(mr)}}{\left[E_m^{(mr)}-E_r^{(mr)}\right]^2},\quad m=\overline{1,N},m\neq r\ . \qquad (6)$$

Проведемо синтез лінійних РП при степені полінома $s=1$, де узагальнені РП для поставленої задачі приймуть вигляд:

$$\Lambda(\mathbf{X})^{(i0)}_{1n}=\sum_{v=1}^{n}k_{1v}^{(i0)}x_v+k_0^{(i0)}\underset{H_0}{\overset{H_i}{\gtrless}}0\ ,\ i=1,2,$$

$$\Lambda(\mathbf{X})^{(21)}_{1n}=\sum_{v=1}^{n}k_{1v}^{(21)}x_v+k_0^{(21)}\underset{H_1}{\overset{H_2}{\gtrless}}0\ . \qquad (7)$$

Показано, що оптимальні коефіцієнти $k_{1v}^{(10)}$, $k_{1v}^{(20)}$, $k_{1v}^{(21)}$ РП (7) знаходяться із рішення системи алгебраїчних рівнянь вигляду (4):

$$k_{1v}^{(10)}=\frac{e_{1v}\sqrt{q_1}}{2\sqrt{\chi_2}},\ k_{1v}^{(20)}=\frac{e_{2v}\sqrt{q_2}}{2\sqrt{\chi_2}},\ k_{1v}^{(21)}=\frac{e_{2v}\sqrt{q_2}-e_{1v}\sqrt{q_1}}{2\sqrt{\chi_2}},$$

де $e_{iv}=r_{iv}\cos(\omega_{0i}v\delta)$, v – номер вибіркового значення, δ – крок дискретизації, $i=1,2$.

Для знаходження граничних коефіцієнтів $k_0^{(10)}$, $k_0^{(20)}$, $k_0^{(21)}$ скористаємося виразом (3). Після нескладних перетворень можемо записати їх остаточний вигляд:

$$k_0^{(10)}=-\frac{1}{4}\sum_{v=1}^{n}e_{1v}^2q_1,\ k_0^{(20)}=-\frac{1}{4}\sum_{v=1}^{n}e_{2v}^2q_2\ ,$$

$$k_0^{(21)}=\frac{1}{4}\sum_{v=1}^{n}\left(e_{1v}^2q_1-e_{2v}^2q_2\right).$$

Тоді РП (7) при степені полінома $s=1$ приймуть остаточний вигляд:

$$\Lambda(\mathbf{X})^{(i0)}_{1n}=\sum_{v=1}^{n}\frac{e_{iv}\sqrt{q_i}}{2\sqrt{\chi_2}}x_v-\frac{1}{4}\sum_{v=1}^{n}e_{iv}^2q_i\underset{H_0}{\overset{H_i}{\gtrless}}0\ ,\ i=1,2\ ,$$

$$\Lambda(\mathbf{X})^{(21)}_{1n}=\sum_{v=1}^{n}\frac{e_{2v}\sqrt{q_2}-e_{1v}\sqrt{q_1}}{2\sqrt{\chi_2}}x_v+\frac{1}{4}\sum_{v=1}^{n}\left(e_{1v}^2q_1-e_{2v}^2q_2\right)\underset{H_1}{\overset{H_2}{\gtrless}}0.$$

У цьому випадку для поставленої задачі розрізнення трьох статистичних гіпотез верхні границі суми

ймовірностей помилок першого та другого роду будуть визначатися значенням критерію якості згідно (6).

Коефіцієнти РП і значення критерію якості при степені полінома $s=1$ не залежать від коефіцієнта асиметрії γ_3 і ексцесу γ_4 та повністю збігаються з відомими результатами [2], коли розглядається адитивна модель радіосигналу та гаусівської завади.

Кількість добутої інформації з вибіркових значень про розрізнення гіпотез $I_{Ku\,1n}^{(mr)}$ є зворотною величиною (6) і обчислюється згідно виразу (5) для РП $\Lambda(\mathbf{X})_{2n}^{(21)}$ і $\Lambda(\mathbf{X})_{2n}^{(i0)}$, $i=1,2$.

Проведемо збільшення степеня полінома до $s=2$, де будуть враховуватися кумулянтні коефіцієнти прийнятої випадкової величини до 4-го порядку при гіпотезі й альтернативах.

У цьому випадку РП, відповідно до узагальненого виразу (2), приймуть вигляд:

$$\Lambda(\mathbf{X})_{2n}^{(i0)}=\sum_{v=1}^{n}k_{1v}^{(i0)}x_v+\sum_{v=1}^{n}k_{2v}^{(i0)}x_v^2+k_0^{(i0)}\underset{H_0}{\overset{H_i}{\gtrless}}0,\ i=1,2, \qquad (8)$$

$$\Lambda(\mathbf{X})_{2n}^{(21)}=\sum_{v=1}^{n}k_{1v}^{(21)}x_v+\sum_{v=1}^{n}k_{2v}^{(21)}x_v^2+k_0^{(21)}\underset{H_1}{\overset{H_2}{\gtrless}}0,$$

де оптимальні коефіцієнти РП $\Lambda(\mathbf{X})_{2n}^{(i0)}$, згідно (3) і (4) дорівнюють:

$$k_0^{(i0)}=\sum_{v=1}^{n}\frac{2e_{iv}^2q_i-2e_{iv}\sqrt{q_i}\gamma_3+e_{iv}^4q_i^2+e_{iv}^2q_i\gamma_4}{4\gamma_3^2-4e_{iv}^2q_i-8-4\gamma_4},$$

$$k_{1v}^{(i0)}=\frac{e_{iv}\sqrt{q_i}\left(2+e_{iv}^2q_i+e_{iv}\sqrt{q_i}\gamma_3+\gamma_4\right)}{2\sqrt{\chi_2}\left(2+e_{iv}^2q_i-\gamma_3^2+\gamma_4\right)},$$

$$k_{2v}^{(i0)}=\frac{-e_{iv}\sqrt{q_i}\gamma_3}{2\left(2+e_{iv}^2q_i-\gamma_3^2+\gamma_4\right)\ \chi_2}.$$

Відповідно, оптимальні коефіцієнти РП (8) $\Lambda(\mathbf{X})_{2n}^{(21)}$, приймуть вигляд:

$$k_0^{(21)}=\sum_{v=1}^{n}\Big(\left(e_{1v}\sqrt{q_1}-e_{2v}\sqrt{q_2}\right)\times$$
$$\times\left(e_{1v}^3q_1^{3/2}+2e_{2v}\sqrt{q_2}-e_{1v}^2e_{2v}q_1\sqrt{q_2}+e_{2v}^3q_2^{3/2}-2\gamma_3-\right.$$
$$-2e_{1v}\sqrt{q_1}\gamma_4+e_{2v}\sqrt{q_2}\gamma_4+e_{1v}\sqrt{q_1}\times$$
$$\left.\times\left(2-e_{2v}\left(e_{2v}q_2+2\sqrt{q_2}\gamma_3\right)\right)/\left(8\left(2+e_{1v}^2q_1-\right.\right.\right.$$
$$\left.\left.\left.-2e_{1v}e_{2v}\sqrt{q_1}\sqrt{q_2}+e_{2v}^2q_2-\gamma_3^2+\gamma_4\right)\right)\Big),$$

$$k_{1v}^{(21)}=-\frac{\left(e_{1v}\sqrt{q_1}-e_{2v}\sqrt{q_2}\right)\left(2+e_{1v}^2q_1+e_{2v}^2q_2+e_{2v}\sqrt{q_2}\gamma_3+e_{1v}\sqrt{q_1}\left(\gamma_3-2e_{2v}\sqrt{q_2}\right)+\gamma_4\right)}{4\left(2+e_{1v}^2q_1-2e_{1v}e_{2v}\sqrt{q_1}\sqrt{q_2}+e_{2v}^2q_2-\gamma_3^2+\gamma_4\right)\ \sqrt{\chi_2}},$$

$$k_{2v}^{(21)}=-\frac{\left(e_{1v}\sqrt{q_1}-e_{2v}\sqrt{q_2}\right)\gamma_3}{4\left(2+e_{1v}^2q_1-2e_{1v}e_{2v}\sqrt{q_1}\sqrt{q_2}+e_{2v}^2q_2-\gamma_3^2+\gamma_4\right)\ \chi_2}.$$

Аналіз коефіцієнтів РП $\Lambda(\mathbf{X})_{2n}^{(21)}$ і $\Lambda(\mathbf{X})_{2n}^{(i0)}$, $i=1,2$ показує, що вони залежать не тільки від параметрів відношення сигнал/шум q_1 і q_2, але й від таких параметрів, як коефіцієнти асиметрії γ_3 та ексцесу γ_4, що характеризують ступінь негаусовості адитивної завади. Знайдені оптимальні коефіцієнти будуть характеризувати й критерій якості $Ku(E,G)_{2n}$ (6), через який оцінюється ефективність поліноміальних РП. Кількість добутої інформації з вибіркових значень про розрізнення гіпотез $I_{Ku\,2n}^{(mr)}$ є зворотною величиною $Ku(E,G)_{2n}$ та обчислюється згідно виразів (5) для РП $\Lambda(\mathbf{X})_{2n}^{(21)}$ і $\Lambda(\mathbf{X})_{2n}^{(i0)}$, $i=1,2$.

Аналогічним чином отримані результати для синтезу РП при степенях полінома $s=\overline{3,6}$, які в силу громіздкості аналітичних виразів не приводяться.

Характерною рисою нових РП є той факт, що вибіркові значення x_v^i піддаються нелінійній обробці та враховується структура випадкових сигналів не тільки у вигляді їхніх дисперсій χ_2, але і кумулянтних коефіцієнтів третього й вищих порядків. Врахування таких параметрів дозволяє описувати випадкові сигнали, розподіл яких відрізняється від нормального.

Досліджено вплив асиметрично-ексцесної негаусівської завади другого типу першого виду на ефективність нелінійних РП розрізнення сигналів. Ефективність оцінювалася по сумарній асимптотичній ймовірності R_s помилок РП розрізнення сигналів (6) для різних поліноміальних перетворень (рис. 4).

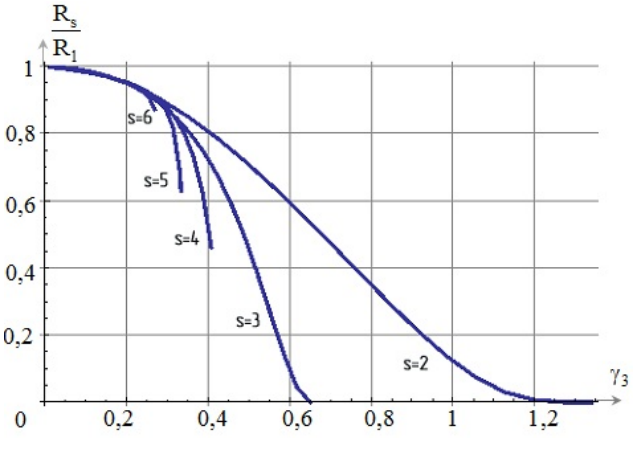


Рис. 4. Відношення суми ймовірностей помилок РП при степені полінома $s=\overline{2,6}$ (R_s) до РП при степені полінома $s=1$ (R_1) від значень коефіцієнта асиметрії γ_3 при різних відношеннях «сигнал-шум» $q_1=1$ і $q_2=2$, $n=100$, $\gamma_4=0$

Відношення R_s/R_1 характеризує ймовірності помилок нелінійних РП при $s=2-6$ до ймовірностей помилок лінійних РП при $s=1$ для різних значень відношень потужностей сигналів і завад $q_r=\frac{a_r^2}{\chi_2}$, $r=1,2$.

З рис. 4 видно, що з урахуванням кумулянтних коефіцієнтів ймовірність помилок нелінійних РП зменшується до значень R_s/R_1 менше одиниці. Максимальне зменшення отримане при досягненні коефіцієнтів γ_3,γ_4 області допустимих значень [6, 7]. При зростанні ступеня

полінома s області допустимих значень параметрів γ_3, γ_4 зменшуються, але ефективність обробки збільшується.

7. Комп'ютерне моделювання поліноміальних алгоритмів обробки сигналів

Використовуючи генератор псевдовипадкових послідовностей, що базуються на бігаусовій моделі [11], як складову частину експериментального комплексу, проведено комп'ютерне моделювання спільних алгоритмів розрізнення сигналів та оцінювання їх параметрів. В якості програмного середовища використано проблемно-орієнтований пакет Matlab 2013.

Моделювання спільних алгоритмів розрізнення та оцінювання проведені при степенях стохастичного полінома $s=1$ та $s=2$ при заданому об'ємі вибірки $n=1000$ та кількості експериментів $k=200$. Результати моделювання представлено у вигляді графіків (рис. 5–7). На рис. 4 зображено теоретичний та експериментальний графіки залежності ефективності нелінійного РП (s=2) розрізнення сигналів по відношенню до лінійного РП (s=1) та оцінюється відношенням кількості добутої інформації $I_{s=1}/I_{s=2}$ з вибіркових значень про розрізнення гіпотез і характеризує ймовірності помилок першого та другого роду.

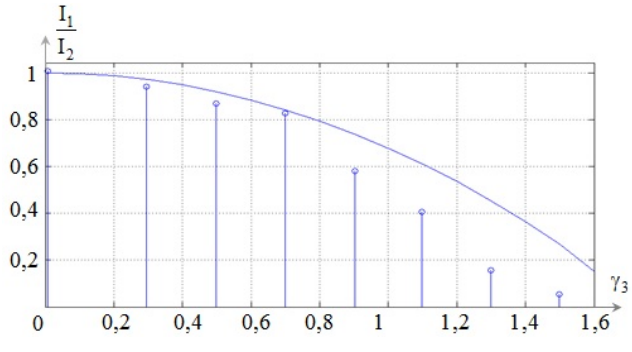


Рис. 5. Залежність ефективності поліноміальних РП при степені полінома $s=1$ до $s=2$ від коефіцієнта асиметрії γ_3, коефіцієнт ексцесу $\gamma_4=0,7$

На рис. 6, *а* представлено теоретичний та експериментальний графіки залежності коефіцієнтів зменшення дисперсій оцінок амплітуди першого радіосигналу $g(a_{01})_{21}$ та частоти другого сигналу $g(\omega_{02})_{21}$ (рис. 6, *б*), що знаходяться як відношення дисперсій отриманих оцінок при різних степенях стохастичного полінома s:

$$g(a_{01})_{21}=\frac{\sigma^2(a_{01})_{s=2}}{\sigma^2(a_{01})_{s=1}},\ g(\omega_{02})_{21}=\frac{\sigma^2(\omega_{02})_{s=2}}{\sigma^2(\omega_{02})_{s=1}}.$$

Залежність інших коефіцієнтів зменшення дисперсій оцінок параметрів радіосигналів мають подібний характер зміни.

Експериментально відношення ефективності поліноміальних РП оцінюється як відношення суми ймовірності помилок для різних степенів полінома $(\alpha+\beta)_{s=2}/(\alpha+\beta)_{s=1}$, де α та β – ймовірності помилок 1-го та 2-го роду відповідно [12]. В табл. 1 наведено ймовірність помилок РП для степенів полінома $s=1$ та $s=2$ при $\gamma_3=1,5$ та $\gamma_4=0,7$.

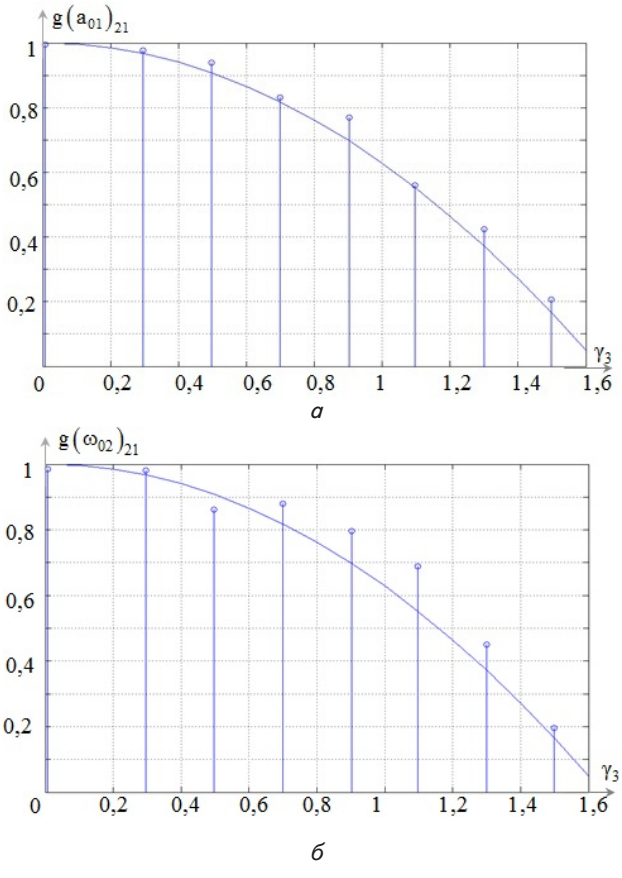


Рис. 6. Залежність коефіцієнта зменшення дисперсій оцінок: *а* – амплітуди першого сигналу $g(a_{01})_{21}$; *б* – частоти другого сигналу $g(\omega_{02})_{21}$ від γ_3, γ_4=0,7

Таблиця 1

Ймовірність помилок поліноміальних РП

№	Помилки	s=1	s=2
1	α^{10} (хибне виявлення 1-го сигналу)	86 %	0,5 %
2	α^{20} (хибне виявлення 2-го сигналу)	36,5 %	0
3	β^{10} (пропуск 1-го сигналу)	0,03 %	0
4	β^{20} (пропуск 2-го сигналу)	35,5 %	0
5	α^{21} (хибне виявлення 2-го сигналу)	21 %	5 %
6	β^{21} (хибне виявлення 1-го сигналу)	20 %	5,5 %

На рис. 7 представлено результати моделювання серії експериментів обробки сигналів на фоні адитивної асиметрично-ексцесної завади лінійним та нелінійним РП.

З графіків видно, що результати обробки лінійним РП (рис. 7, *а*) (який є оптимальним для гаусівських завад) вибіркових значень сигналу при негаусівських завадах характеризуються більш частими хаотичними викидами і перевищеннями нульового порогу в порівнянні з результатами обробки нелінійним РП (рис. 7, *б*), який враховує коефіцієнти третього та четвертого порядків.

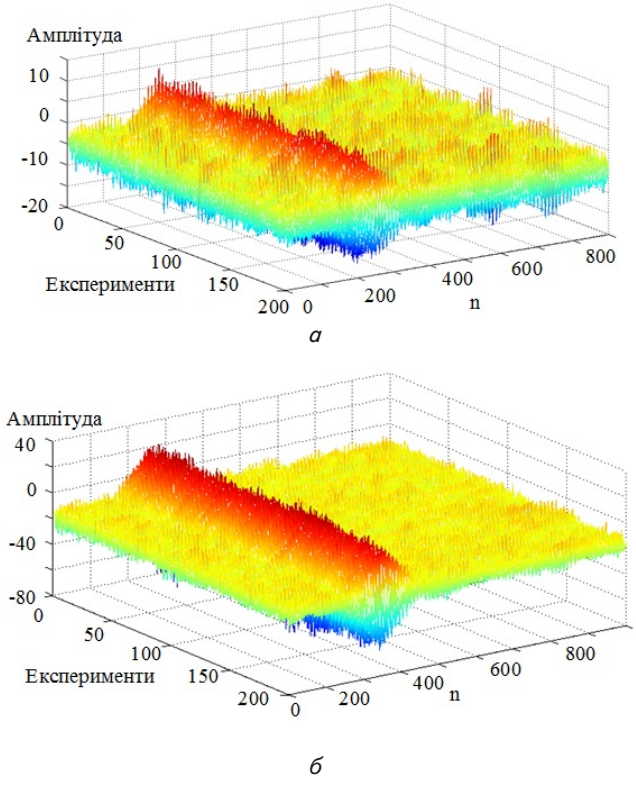


Рис. 7. Результат обробки вибіркових значень: *а* – лінійним РП; *б* – нелінійним РП при $\gamma_3 = 1{,}5$ та $\gamma_4 = 0{,}7$

8. Висновки

Показано, що при лінійній обробці вибіркових значень ($s=1$) отримуються рішення, які повністю співпадають з відомими підходами обробки сигналів при використанні гаусівських моделей випадкових величин. При нелінійній обробці ($s \geq 2$) враховується статистика третього і вище порядків у вигляді коефіцієнтів асиметрії, ексцесу, що дає можливість описувати ступінь негаусовості запропонованих моделей випадкових величин. Врахування таких параметрів дозволяє суттєво покращити результати оцінювання параметрів у вигляді зменшення дисперсії оціночних значень та зменшити ймовірності помилок поліноміальних РП в порівнянні з відомими результатами.

Експериментально отримані результати комп'ютерного моделювання алгоритмів спільного розрізнення радіосигналів та оцінювання їх параметрів в цілому відповідають теоретичним. Співпадання експериментальних результатів з теоретичними відбуватиметься при збільшенні об'єму вибірки n та кількості проведених експериментів k. Встановлено, що ефективність поліноміальних алгоритмів розрізнення та оцінювання підвищується зі збільшенням степеня стохастичного полінома та по мірі наближення значення коефіцієнтів асиметрії та ексцесу до границі області допустимих значень, тобто ймовірність помилок першого і другого роду та дисперсії отриманих оцінок зменшуються.

Отже, в результаті дослідження сформовано моментні критерії якості перевірки статистичних гіпотез, поліноміальні розв'язувальні правила та поліноміальні алгоритми спільного оцінювання параметрів випадкових величин. Побудовано ефективні методи і комп'ютерні засоби функціонування систем прийому та обробки даних відповідного класу.

Отримані результати можуть бути використані для зменшення ймовірності помилок розрізнення радіосигналів та підвищення точності оцінок їх параметрів в радіолокації, радіонавігації та інших сферах, де точність алгоритмів обробки сигналів відіграє важливу роль.

Література

1. Трифонов, А. П. Совместное различение сигналов и оценка их параметров на фоне помех [Текст] / А. П. Трифонов, Ю. С. Шинаков. – М.: Радио и связь, 1986. – 264 с.
2. Van Trees, H. L. Detection Estimation and Modulation Theory [Text] / H. L. Van Trees, K. L. Bell, Z. Tiany; 2nd ed. – John Wiley & Sons, 2013. – 1176 p.
3. Литвин-Попович, А. И. Обнаружение сигналов и измерение их параметров в следящих радиотехнических системах [Текст] / А. И. Литвин-Попович // Технологический аудит и резервы производства. – 2013. – Т. 6, № 1(14). – С. 30–34.
4. Sobolev, V. S. Maximum-likelihood estimates of the frequency of signals of laser Doppler anemometers [Text] / V. S. Sobolev, F. A. Zhuravel' // Journal of Communications Technology and Electronics. – 2014. – Vol. 59, Issue 4. – P. 294–301. doi: 10.1134/S1064226914030103
5. Krupiński, R. Modified Moment Method Estimator for the Shape Parameter of Generalized Gaussian Distribution for a Small Sample Size [Text] / R. Krupiński // Computer Information Systems and Industrial Management. – 2013. – Vol. 8104. – P. 420–429. doi: 10.1007/978-3-642-40925-7_39
6. Kunchenko, Y. P. Polynomial Parameter Estimations of Close to Gaussian Random Variables [Text] / Y. P. Kunchenko. – Aachen: Shaker Verlag, 2002. – 396 p.
7. Малахов, А. Н. Кумулянтный анализ негауссовских процессов и их преобразований [Текст] / А. Н. Малахов – М.: Сов. радио, 1979. – 376 с.
8. Палагін, В. В. Нелінійні алгоритми виявлення радіосигналів на тлі адитивно–мультиплікативних негаусівських завад [Текст] / В. В. Палагін // Східно-Європейський журнал передових технологій. – 2012. – Т. 6, № 11(60) – С. 23–28.
9. Палагін, В. В. Розпізнавання радіосигналів на тлі асиметричних негауссівських завад за моментним критерієм якості [Текст] / В. В. Палагін, О. М. Жила // Міжвідомчий науково-технічний збірник «Електромашинобудування та електрообладнання». – 2009. – Вип. №73. –С. 125–130.

10. Гончаров, А. В. Оцінка амплітуди радіосигналу при асиметрично-ексцесній адитивній заваді із застосуванням усічених поліномів Кунченка [Текст] / А. В. Гончаров, В. М. Уманець // Вісник ЧДТУ – 2013. – № 2. – С. 111–118.
11. Кунченко, Ю. П. Генерація псевдовипадкових послідовностей на основі бігаусового розподілу [Текст] / Ю. П. Кунченко, С. В. Заболотній, О. С. Гавриш, А. Ю Іванченко// Комп'ютерні технології друкарства. – 2000. – № 4. – С. 343–351.
12. Палагін, В. В. Комп'ютерне моделювання сумісних алгоритмів розрізнення радіосигналів та оцінювання їх параметрів на фоні негаусівських завад [Текст] / В. В. Палагін, А. В. Гончаров, В. М. Уманець // PREDT-2013: праці III міжнародної науково-практичної конференції, 24-26 жовтня 2013 р.: тези доп. – Чернівці: ЧНУ імені Юрія Федьковича, 2013. – С. 109–110.

Розглядаються структура, базові перетворення та режими застосування перспективного криптографічного алгоритму симетричного блокового перетворення «Калина». Досліджуються математичні та програмні моделі криптоалгоритму для перевірки правильності реалізації. Для виключення джерела загальних помилок у різних компонентах шифру застосовується багатоверсійна розробка. Обґрунтовується методика перевірки правильності програмної реалізації криптографічного перетворення включаючи режими застосування та тестові приклади

Ключові слова: блоковий симетричний шифр, криптографічне перетворення, правильність програмної реалізації, тестові приклади

Рассматриваются структура, базовые преобразования и режимы использования перспективного криптографического алгоритма симметричного блочного преобразования «Калина». Исследуются математические и программные модели криптоалгоритма для проверки правильности реализации. Для исключения источники общих ошибок в различных компонентах шифра применяется многоверсионная разработка. Обосновывается методика проверки правильности программной реализации криптографического преобразования включая режимы применения и тестовые примеры

Ключевые слова: блочный симметричный шифр, криптографическое преобразование, правильность программной реализации, тестовые примеры

УДК 004.056.55
DOI:10.15587/1729-4061.2014.28010

РОЗРОБКА МАТЕМАТИЧНИХ ТА ПРОГРАМНИХ МОДЕЛЕЙ ПЕРСПЕКТИВНОГО АЛГОРИТМУ ШИФРУВАННЯ ДЛЯ ПЕРЕВІРКИ ПРАВИЛЬНОСТІ РЕАЛІЗАЦІЇ

Ю. І. Горбенко
Кандидат технічних наук, старший науковий співробітник, лауреат державної премії в галузі науки та техніки*
E-mail: GorbenkoU@iit.com.ua
Р. І. Мордвінов
Аспірант*
E-mail: RMordvinov@gmail.com
О. О. Кузнецов
Доктор технічних наук, професор
Кафедра безпеки інформаційних систем та технологій
Харківський національний університет ім. В. Н. Каразіна
пл. Свободи, 4, м. Харків, Україна, 61022
E-mail: kuznetsov_alex@rambler.ru
*Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
пр. Леніна, 14, м. Харків, Україна, 61000

1. Вступ

Важливою складовою безпеки сучасних інформаційно-комунікаційних систем є механізми криптографічного захисту, зокрема блокове симетричне шифрування (БСШ), яке полягає у перетворенні інформації з використанням ключових даних з метою приховування (відновлення) змісту інформаційного повідомлення, підтвердження його справжності, цілісності, авторства.

У напрямку розроблення вітчизняних методів і засобів захисту інформації для забезпечення взаємної