МЕТОДЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 681.3.07 (3.06)

О.П. НАРЄЖНІЙ, канд. техн. наук, В.В. СЕМЕНЕЦЬ, д-р техн. наук,
Т.О. ГРІНЕНКО, канд. техн. наук

МЕТОД ВИМІРЮВАННЯ КВАНТОВОГО ФАЗОВОГО ШУМУ ТА ШИРИНИ ЛІНІЇ РОБОЧОГО ПЕРЕХОДУ РАДІООПТИЧНОЇ СИСТЕМИ ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

Вступ

Такі важливі питання квантової інформації, як квантові шуми, квантова корекція помилок, числові параметри квантової інформації (ентропія фон Неймана, пропускна здатність квантового каналу зв'язку та інші) знаходяться в стадії інтенсивних експериментальних та теоретичних досліджень [1, 2]. Методологія і теоретична база вивчення проблем вимірювання квантових шумів, що виникають при проектуванні і створенні апаратно-програмних реалізацій квантових генераторів випадкових чисел (КГВЧ), в даний час тільки формуються.

Важливим напрямком досліджень є питання реалізації та використання методів метрологічних досліджень за допомогою сучасної еталонної бази на різних етапах генерування випадкових послідовностей та верифікації квантових генераторів. Останні дослідження дозволили припустити, що одними із найбільш переважних є методи генерування випадкових послідовностей, що ґрунтуються на фізичному джерелі випадковості з використанням елементарних квантово-механічних рішень. В загальному розумінні поява кожного окремого результату такого квантово-механічного рішення є об'єктивно випадковою (невизначуваною, невідомою). Існує ряд елементарних методів (рішень) генерування випадкових послідовностей, які можна використовувати в якості джерел випадковості. Серед основних механізмів генерування ключів слід виділити такі [2 – 20]: метод розщеплення одиничного фотона на два шляхи та поляризації одиничного фотона; метод виявлення заплутаності шляху числа фотонів; методи підрахунку часу генерації або кількості фотонів; використання гомодинного виявлення флуктуації вакуумного стану; інтерферометричні схеми; використання методу подвійного радіооптичного резонансу (ПРР) в парах лужних металів [20].

В роботі [20] розроблено систему компарування для вимірювання фази коливань та квантових фазових шумів. Експеримент з генерації випадкових чисел методом ПРР здійснювався на основі метрологічних методів експериментального дослідження квантових генераторів шумів та квантових мір частоти (КМЧ). Висока стабільність КМЧ дозволяє стабілізувати фазу КГВЧ регулюванням його опорної частоти. При цьому проста і надійна конструкція такого генератора припускає його практичне застосування.

Мета статті – обґрунтування методу вимірювання квантового фазового шуму та ширини лінії робочого переходу радіооптичної системи генератора випадкових чисел (ГВЧ), що базується на методі подвійного радіооптичного резонансу.

Основна частина

Побудова перспективного КГВЧ на основі методу ПРР вимагає з'ясування оптимальних умов процесу оптичної накачки з точки зору отримання максимального параметра якості квантових дискримінаторів (КД). Для цього розраховують параметр якості при накачуванні атомів Rb^{87} природним світлом з урахуванням релаксаційних процесів, спектрального складу і поглинання світла накачування. Інтенсивність квантового фазового шуму є однією з найважливіших метрологічних характеристик КГВЧ як генератора шуму. Відомо [20], що серед усіх можливих типів шумів у схемі оптичного накачування і детектування резонансу прин-

ципово квантову природу мають тільки два типи шумів – дробовий шум світла і квантовий шум атомного ансамблю. Метод ПРР базується на двох складових: перша – це селективне оптичне збудження, що приводить до появи збуджених атомів, які нерівномірно заселяють підрівні збудженого стану; друга – це індукування радіочастотних переходів з допомогою допоміжного змінного поля і реєстрація цих переходів у оптичному каналі (подвійний резонанс названий подвійним, тому що є два види резонансу – на оптичних частотах і на радіочастоті).

Ширину лінії КД на парах лужних металів можна розглядати як наслідок випадкового фазового коливання оптичного поля. Залежність ширини лінії КД від вихідної потужності спектрального джерела лампи або лазера потребує розроблення теоретичної моделі генерації випадкових чисел. На практиці існують фактори, які важко враховувати при проведенні вимірювань методами інтерферометричного експерименту оптичної фази поля КД. Тому використання в якості джерела квантового фазового шуму КД на парах лужних металів потребує проведення експериментальних досліджень за допомогою сучасних еталонних КМЧ. При цьому необхідною умовою для генерації випадкових чисел за допомогою КД на парах лужних металів є стабілізація частоти вимірювання.

При визначенні параметрів квантових фазових шумів вихідного сигналу КГВЧ, що реалізований за допомогою методу ПРР, можна застосовувати два методи виміру – двогенераторний і тригенераторний. В роботі [20] при настроюванні та регулюванні перспективного КГВЧ використовувався метод групового еталонування за допомогою КМЧ. При цьому поряд з удосконалюванням самих методів вимірювання виникає необхідність розробляти математичні моделі, що враховують вплив різних дестабілізуючих факторів на флуктуації фази (частоти) ГВЧ.

У загальному випадку побудовою даних моделей займається теорія флуктуацій в автоколивальних системах. Найважливішим її розділом, що виділився за останні два десятиліття в самостійний напрямок, є теорія флуктуацій частоти квантових автогенераторів, що виявляє причини, характер і статистичні характеристики випадкових відхилень опорної частоти від її сталого значення [21]. При цьому облік впливу дестабілізуючих факторів пов'язаний з відомими труднощами, обумовленими їх різноманітністю не тільки по виду, але й по інтенсивності, напрямку дії, спектру тощо. Так, облік магнітного та електромагнітного впливів має важливе значення для пасивних КМЧ. Це обумовлено тим, що принцип дії квантових дискримінаторів побудований на розщепленні в магнітному полі надтонких рівнів квантових переходів з підбором такого значення магнітного поля, при якому частота генерованих кварцевим генератором коливань стає кратною номінальному значенню частоти. Крім стохастичної зміни магнітного та електромагнітного полів, можлива й квазирегулярна їх зміна, яка може впливати на стабільність частоти та фази вихідного сигналу КГВЧ. Зокрема, така ситуація має місце при об'єднанні пасивних КМЧ у груповий еталон часу та частоти. По суті, взаємний вплив КМЧ у групі еквівалентний тому, що кожна міра зазнає деякий зовнішній вплив з боку інших мір групи. І, оскільки такий вплив взаємний, то його результатом повинен бути якийсь векторний процес із взаємною кореляцією між його елементами. Це призводить до необхідності пошуку нових методів стабілізації частоти КГВЧ на основі використання інформації про залежність поведінки частоти вихідного сигналу з урахуванням похибки від взаємодії.

Проте, у теорії флуктуацій частоти квантових автогенераторів не розглядалися питання, пов'язані з вивченням їх взаємодії (взаємозв'язку), тобто опускалися питання впливу похибки від взаємодії на інтенсивність флуктуацій частоти. Це пов'язано з тим, що апріорі передбачається можливість компенсації даної похибки апаратними засобами. Тому усі відомі методи оцінки інтенсивності частотних (фазових) флуктуацій і експериментальні методи виміру нестабільності частоти: фазовий, інтерференційний, лічильно-імпульсний та ін., засновані на базовому припущенні про відсутність взаємних впливів КМЧ у процесі вимірювань.

Крім того, на основі результатів, отриманих у роботах [22, 23], можна стверджувати, що задача ідентифікації КГВЧ за результатами вимірювань належить до класу некоректних задач математичної фізики й вимагає рішення спеціальних питань – пошуку й визначення регуляризовувальних параметрів або факторів, що дозволяють одержувати стійкі рішення диференціальних рівнянь, які описують поведінку вихідних сигналів даних мір.

Звідси випливає така постановка задачі: розробити методику регуляризації задачі ідентифікації групи КМЧ та КГВЧ за наявності похибки від взаємодії через канали звірення з обліком їх адитивних внутрішніх шумів на основі застосування статистичних методів рішення двоточечних крайових завдань; обґрунтувати перетворення вектора стану групи КМЧ як неспостережуваного процесу до спостережуваного на основі стохастичної моделі системи пов'язаних осциляторів.

Оскільки для одержання оцінок поточних значень фаз вихідних сигналів КМЧ доводиться мати справу з диференціальними рівняннями, інтегрування яких класичними методами неможливо (тобто є некоректні задачі математичної фізики, що вимагають процедур регуляризації), найбільший інтерес у цьому випадку представляють статистичні методи рішення двоточечних крайових завдань. Одним з таких методів є метод фільтра Калмана, що здійснює статистичне згладжування рішень і, за певних вимог до параметрів розглянутої моделі, є асимптотично стійким. Проте, поряд з високою точністю, даний метод використовує й найбільшу кількість апріорної інформації: коваріацію помилок і математичного очікування правої частини й рішення [23]. Для отримання даної апріорної інформації будемо розглядати груповий еталон з позицій теорії нелінійних автоколивальних систем із близькими частотами. При цьому необхідно побудувати модель зміни фази (частоти) групового еталону як стохастичну модель системи пов'язаних осциляторів (мір частоти).

У роботі [24] показано, що зміна фази (повільна у порівнянні з періодом коливань) вихідного сигналу кожної міри в групі з N мір за наявності їх взаємодії може бути представлена диференціальним рівнянням

$$\dot{\psi}_i(t) = \Delta\omega_i + \sum_{\substack{j=1 \\ j\neq i}}^{N} \left[\frac{\alpha_{ij}}{2} \frac{A_j}{A_i} \cos\phi_{ij}(t) \right] + \xi_i(t), \qquad (1)$$

де A_j та A_i – амплітуди коливань вихідних сигналів *j*-ї та *i*-ї міри відповідно; α_{ij} – коефіцієнт електричного зв'язку між мірами та КГВЧ; $\phi_{ij}(t) = \psi_i(t) - \psi_j(t)$ – різниця фаз коливань вихідних сигналів, генерованих *i*-ю та *j*-ю мірами та КГВЧ; $\xi_i(t)$ – власні флуктуації частоти вихідного сигналу *i*-ї міри з математичним очікуванням $M[\xi_i(t)] = 0$ і кореляційною функцією $M[\xi_i(t)\xi_i(t+\tau)] = \sigma_i^2\delta(\tau)$ ($\delta(\tau)$ – дельта-функція, а σ_i – середнє квадратичне відхилення (СКВ) флуктуацій вихідного сигналу *i*-ї КМЧ); $\Delta\omega_i$ – відхилення частоти *i*-ї міри від номінального значення, кількісна оцінка якого може бути здійснена шляхом звірення вихідного сигналу даної міри з еталонними сигналами часу й частоти, переданими спеціальними системами.

У процесі взаємних звірень КМЧ вимірам піддаються різниці фаз $\phi_{ij}(t)$ або різниці частот $\dot{\phi}_{ij}(t)$ залежно від типу використовуваних компараторів. Вимірювання процесу $\psi_i(t)$ в групі, що складається із КМЧ однакової точності (як правило, найвищої), неможливе, тобто процес $\psi_i(t)$ є принципово неспостережуваним. Тому рішенням задачі ідентифікації групового еталону з максимально можливою точністю є розробка методик ідентифікації поточного стану процесу $\psi_i(t)$ за результатами вимірювань процесів $\phi_{ij}(t)$ або $\dot{\phi}_{ij}(t)$ з наступною компенсацією взаємного впливу КМЧ та КГВЧ. Дотримуючись мети даного завдання, систему рівнянь (1) щодо вимірюваних параметрів можна перетворити таким чином:

$$\dot{\phi}_{ij}(t) = \Delta_{ij} + \sum_{\substack{n=1 \\ n\neq i}}^{N} A_{in}\cos\phi_{in}(t) - \sum_{\substack{m=1 \\ m\neq j}}^{N} A_{jm}\cos\phi_{jm}(t) + (\xi_i - \xi_j), \quad (2)$$

де $\Delta_{ij} = (\Delta\omega_i - \Delta\omega_j)$ – різниця частот між *i*-ю та *j*-ю КМЧ та КГВЧ; $A_{in} = \frac{\alpha_{in}}{2}\frac{A_n}{A_i}$ – узагальнене значення амплітуди, обумовлене похибкою від взаємодії *i*-ї та *n*-ї мір; $A_{jm} = \frac{\alpha_{jm}}{2}\frac{A_m}{A_j}$ – аналогічно для *j*-ї та *m*-ї мір.

Залежно від співвідношення параметрів Δ_{ij}, $A_{ij} = \frac{\alpha_{ij}}{2}\frac{A_j}{A_i}$ і $\sigma_{ij} = \sqrt{\sigma_i^2 + \sigma_j^2}$ система рівнянь (2) допускає різні типи рішень. Якщо $\Delta_{ij} \le \sum_{\substack{n=1 \\ n\neq i}}^{N} |\alpha_{in}| + \sum_{\substack{m=1 \\ m\neq j}}^{N} |\alpha_{jm}|$, система рівнянь стає виродженою щодо членів з індексами *ij* та *ji*. Фізично це виявляється у тому, що відбувається взаємна синхронізація КМЧ із номерами *i* та *j*, у результаті чого вони поводяться як одне ціле. А за виконання умови $\Delta_{ij} > \sum_{\substack{n=1 \\ n\neq i}}^{N} |\alpha_{in}| + \sum_{\substack{m=1 \\ m\neq j}}^{N} |\alpha_{jm}|$ між усіма КМЧ виникає режим амплітудних биттів. При цьому задача ідентифікації групового еталону (оцінки фази КМЧ та КГВЧ) не є коректною в класичному сенсі (за Адамаром) [25, 26]. Проте, у роботі [24] показано, що для випадку знаходження усіх КМЧ групи та КГВЧ в режимі биттів, методами розщеплення вдається зробити редукцію даної задачі до суми більш простих, умовно коректних задач математичної фізики.

Для отримання апріорної інформації про тип регулярної складової рішення в режимі биттів КМЧ та КГВЧ скористаємося методом послідовних наближень (метод Крилова – Боголюбова) [27]. Припускаючи, що власні флуктуації частоти усіх КМЧ дорівнюють нулю, послідовне наближення рішення рівняння (2) і відповідно (1) буде відбуватися таким чином.

Початкове наближення обираємо у вигляді: $\tilde{\phi}_{ij,0}(t) = \Delta_{ij}t$, де $\tilde{\phi}_{ij,0}(t)$ – початкове наближення регулярної складової різниці фаз коливань $\phi_{ij}(t)$.

Тоді перше наближення рішення системи (1) щодо регулярної складової зміни фази вихідного сигналу *i*-ї міри

$$\tilde{\psi}_{i,1}(t) = \Delta\omega_i t + \sum_{\substack{j=1 \\ j\neq i}}^{N} A_{ij}\sin(\Delta_{ij}t + \varphi_{0i}), \quad (3)$$

і, відповідно, перше наближення рішення системи (2) щодо регулярної складової різниці фаз коливань між *i*-ю та *j*-ю мірами:

$$\tilde{\phi}_{ij,1}(t) = \Delta_{ij}t + \sum_{\substack{n=1 \\ n\neq i}}^{N} A_{in}\sin(\Delta_{in}t + \vartheta_{0in}) - \sum_{\substack{m=1 \\ m\neq j}}^{N} A_{jm}\sin(\Delta_{jm}t + \vartheta_{0jm}), \quad (4)$$

де φ_{0i} – початкова фаза *i*-ї КМЧ; ϑ_{0in} – різниця початкових фаз між *i*-ю та *n*-ю мірами.

Друге наближення рішення рівняння (2):

$$\tilde{\psi}_{i,2}(t) = \Delta\omega_i t + \sum_{\substack{j=1 \\ j\neq i}}^{N} A_{ij} \sin\left(\Delta_{ij} t + \varphi_{0i}\right) +$$

$$+ \sum_{\substack{j=1 \\ j\neq i}}^{N} A_{ij} \left\{ \sum_{\substack{n=1 \\ n\neq i}}^{N} A_{in} \left[\frac{\cos\left(\Delta_{jn} t + \vartheta_{0in}\right)}{\Delta_{jn}} - \frac{\cos\left(\Delta_{ij} t + \Delta_{in} t + \vartheta_{0in}\right)}{\Delta_{ij} + \Delta_{in}} \right] + \right.$$

$$\left. + \sum_{\substack{m=1 \\ m\neq j}}^{N} A_{jm} \left[\frac{\cos\left(\Delta_{im} t + \vartheta_{0\,jm}\right)}{\Delta_{im}} - \frac{\cos\left(\Delta_{ij} t + \Delta_{jm} t + \vartheta_{0\,jm}\right)}{\Delta_{ij} + \Delta_{jm}} \right] \right\}. \qquad (5)$$

Аналогічно записуються наступні ітерації рішення рівнянь (2) і (3). З (5) виходить, що кожне наступне наближення породжує появу майже періодичних складових рішення на нових комбінаційних частотах. Тому в спектрі випадкового процесу, утвореного з безперервного ряду вимірювань різниць частот (фаз) звірюваних мір, присутні "яскраві" спектральні лінії, породжені взаємним впливом вихідних сигналів на частотах аналізу, приблизно рівних різницям частот $\Delta_{ij} \approx 10^{-p}$ рад/с, де $p \geq 4$ для КМЧ. Спектральна густина потужності фазових флуктуацій на цих частотах буде дорівнювати величині A_{in}^2. Вплив даних квазигармонійних складових на загальну поведінку фаз вихідних сигналів КМЧ залежить від співвідношення Δ_{ij} й A_{in}. В [28] запропоновано спосіб ідентифікації необхідного типу рішення (відповідного режиму взаємодії КМЧ – режиму биттів) за експериментальними даними в спектральній області.

При цьому використання рівняння (1) як рівняння стану в методі фільтра Калмана недоцільно, тому що вимірюванням з необхідною точністю можуть бути піддані тільки різниці фаз $\phi_{ij}(t)$ вихідних сигналів КМЧ. Як показано в [29], матриця вимірювань, що описує процес взаємних звірень мір частоти й часу за допомогою компараторів, така, що умова спостереження не виконується (ранг матриці вимірювань на одиницю менше кількості КМЧ, задіяних у групі). Тому використання стандартних методик лінійної алгебри у фільтрі Калмана призведе до нестійкості одержуваних з його допомогою рішень. Спостережуваним є тільки рівняння стану (2).

Методики визначення кількісних значень Δ_{ij}, A_{ij} і початкових значень різниці фаз $\phi_{ij}(0)$ наведено в [29]. Рівняння (1) і (2) при переході до кінцевих різниць перетворяться відповідно до вигляду

$$\psi_i(k+1) = \psi_i(k) + \Delta\omega_i \tau + \sum_{\substack{j=1 \\ j\neq i}}^{N} \tau A_{ij} \cos\phi_{ij}(k) + \bar{\xi}_i(k); \qquad (6)$$

$$\phi_{ij}(k+1) = \phi_{ij}(k) + \tau\Delta_{ij} + \sum_{\substack{n=1 \\ n\neq i}}^{N} \tau A_{in} \cos\phi_{in}(k) - \sum_{\substack{m=1 \\ m\neq j}}^{N} \tau A_{jm} \cos\phi_{jm}(k) + \bar{\zeta}_{ij}(k), \qquad (7)$$

де τ – інтервал вимірювання різниць фаз $\phi_{ij}(k\tau)$ вихідних сигналів КМЧ та КГВЧ компаратора-

ми $\bar{\zeta}_{ij}(k) = \int_{k\tau}^{(k+1)\tau} \zeta_{ij}(t)dt$; $\bar{\xi}_i(k) = \int_{k\tau}^{(k+1)\tau} \xi_i(t)dt$ – середні значення відповідних шумів на інтерва-

лі вимірювання τ, інтеграли від випадкового процесу розуміються в сенсі, наведеному у роботі [23].

Відповідно до теореми Байеса, умовне середнє значення $\psi_i(k+1|k)$ i-ї КМЧ на $k+1$ кроці ітерації однозначно може бути визначене через умовне середнє значення $\phi_{ij}(k|k)$, оцінене за допомогою методу фільтра Калмана за результатами вимірювань різниці фаз $\phi_{ij}(k)$ на k-му інтервалі вимірювань, і через умовне середнє значення $\psi_i(k|k)$, оцінене на k-му кроці ітерації з виразу

$$\psi_i(k+1|k)=\psi_i(k|k)+\Delta\omega_i\tau+\sum_{\substack{j=1\\ j\neq i}}^{N}\tau A_{ij}\cos\phi_{ij}(k|k). \qquad (8)$$

При цьому, відповідно до теореми Байеса дана оцінка буде оптимальною. Для отримання оцінок поточного значення різниці фаз $\phi_{ij}(k)$ застосуємо метод фільтра Калмана як наслідок спостереження системи, рівняння стану якої описується рівнянням (7), а рівняння вимірювання – вектором виду

$$\vec{Y}(k)=\vec{\Phi}(k)+\vec{\eta}(k),$$

де $\vec{Y}(k)=\left[y_{ij}(k)\right]$ – вектор результатів вимірювань вектора різниці фаз $\vec{\Phi}(k)=\left[\phi_{ij}(k)\right]$; $\vec{\eta}(k)=\left[\overline{\eta}_i(k)\right]$ – вектор власної флуктуації фаз вимірювачів (компараторів) з математичним очікуванням $M\left[\vec{\eta}(k)\right]=0$ і кореляційною функцією $M\left[\vec{\eta}(k)\vec{\eta}(k+1)^T\right]=R\,\delta(\tau)$.

Тоді можна стверджувати, що з точністю до векторної константи $\vec{\Psi}(0)=\left[\psi_i(0)\right]$ можна одержати оптимальні оцінки поточних значень фаз вихідних сигналів усіх КМЧ та КГВЧ, що входять до складу групи.

Проведемо аналіз можливих підходів до регуляризацій процедури оцінки поточних значень різниць фаз між мірами за допомогою нелінійного фільтру Калмана. Так, рівняння (7), що визначає поведінку випадкового процесу різниці фаз у часі, відносить некоректну за Адамаром задачу оцінки $\phi_{ij}(k)$ до класу рішень рівнянь нелінійної фільтрації. Алгоритми нелінійної фільтрації базуються на одному з двох основних регуляризовувальних підходів: на локальній або на інтегральній апроксимації.

Клас наближених алгоритмів фільтрації на основі локальної апроксимації "точного" рішення нелінійного рівняння стану дозволяє одержувати оцінюване значення шуканої величини лише в малій області її варіації.

На відміну від локальної апроксимації, застосовної при малих похибках фільтрації, основна мета інтегральної (глобальної) апроксимації полягає в одержанні наближеного рішення в усій області можливих значень параметра, що фільтрується (шуканого процесу). Це особливо важливо при малих співвідношеннях сигнал/шум, а також у задачах, пов'язаних з виходом процесу за межі заданої області (СКВ випадкового процесу щодо свого умовного середнього).

Локальна апроксимація більш проста в реалізації й використовується у тих випадках, коли очікуване рішення (умовне середнє) є гладкою, повільно мінливою в часі функцією в порівнянні з кроком квантування розглянутого дискретного випадкового процесу. У тих випадках, коли очікуване рішення є функцією, що швидко змінюється, або має розриви першого роду, кращим є використання глобальної апроксимації.

З урахуванням цього звернемось до результатів моделювання процесів зміни фаз вихідних сигналів мір частоти, обумовлених їх взаємним впливом, проведеним в [30]. При аналізі видів рішень, що допускаються рівнянням (1) для взаємодії пари КМЧ і відповідно (7), що є його аналогом для випадку парної взаємодії групи мір, було показано, що дане рівняння

допускає різні типи рішень, умовне середнє, яке може бути як гладкою, повільно мінливою функцією часу, так і функцією, що має квазістрибкоподібну (у порівнянні з інтервалом дискретизації процесу) зміну в часі залежно від співвідношення параметрів.

В [30] наведено такі можливі режими взаємодії: 1 – режим твердої синхронізації; 2 – режим синхронізму з наявністю квазістрибкоподібних змін різниці фаз, що виникають у випадкові моменти часу; 3 – режим биттів; 4 – випадковий процес із лінійним дрейфом різниці фаз. Показано, що першому, третьому й четвертому режимам властиве гладке поводження в часі умовного середнього, тобто при роботі групового еталону в одному з цих режимів доцільним є застосування локальної апроксимації. За наявності хоча б однієї пари мір в групі, що працює в другому режимі, необхідне застосування інтегральної апроксимації.

Розглянемо процедуру лінеаризації нелінійного фільтра Калмана для оцінки поточних значень різниць фаз між мірами на основі стохастичної моделі системи пов'язаних осциляторів. З рівняння (7) виходить, що поточне значення вектора стану $\vec{\Phi}(k)$ формується під впливом двох процесів, породжених однією причиною – взаємодією мір між собою. Перший векторний процес, обумовлений наявністю різниці частот між взаємодіючими мірами та КГВЧ й ефектом перетворення (амплітудно-фазової конверсії) амплітудних биттів у частотні биття, визначає зміну умовного середнього. Другий векторний процес є чисто стохастичним і описує взаємну кореляцію адитивних шумів взаємодіючих мір. Передбачається, що даний процес обумовлений проникненням шумів вихідних сигналів кожної КМЧ та КГВЧ у радіочастотні сигнали їх квантових дискримінаторів.

Це дозволяє зобразити поточний вектор стану у вигляді

$$\vec{\Phi}(k) = \tilde{\vec{\Phi}}(k) + \hat{\vec{\Phi}}(k), \tag{9}$$

де $\tilde{\vec{\Phi}}(k) = \left[\tilde{\phi}_{ij}(k)\right]$ – вектор регулярних складових різниці фаз вихідних сигналів КМЧ та КГВЧ; $\hat{\vec{\Phi}}(k) = \left[\hat{\phi}_{ij}(k)\right]$ – вектор стохастичної складової різниці фаз вихідних сигналів КМЧ та КГВЧ, методологія ідентифікації якого описана в [24].

Підставляння (9) в (7) призводить до того, що рівняння (7) саме стає суперпозицією двох рівнянь, кожне з яких визначає внесок попереднього стану складових процесів (детермінованого і стохастичного) у поточний стан (10). Зважаючи на те, що аналізується стаціонарний режим роботи групової міри, а також те, що в стаціонарному режимі варіація $\hat{\phi}_{ij}(k) << 2\pi$ є незначною, систему (10) можна лінеаризувати розкладанням правої частини в ряд Тейлора відносно $\tilde{\phi}_{ij}(k)$ до лінійного (першого) члену (11)

$$\tilde{\phi}_{ij}(k+1) + \hat{\phi}_{ij}(k+1) = \tilde{\phi}_{ij}(k) + \tilde{\phi}_{ij}(k) + \tau\Delta_{ij} + \sum_{\substack{n=1 \\ n\neq i}}^{N} \tau A_{in} \cos\left[\tilde{\phi}_{in}(k) + \hat{\phi}_{in}(k)\right] -$$

$$- \sum_{\substack{m=1 \\ m\neq j}}^{N} \tau A_{jm} \cos\left[\tilde{\phi}_{jm}(k) + \hat{\phi}_{jm}(k)\right] + \bar{\zeta}_{ij}(k). \tag{10}$$

$$\hat{\phi}_{ij}(k+1) = \hat{\phi}_{ij}(k) + \tilde{\phi}_{ij}(k) + \tau\Delta_{ij} - \tilde{\phi}_{ij}(k+1) + \sum_{\substack{n=1 \\ n\neq i}}^{N} \tau A_{in} \left[\cos\tilde{\phi}_{in}(k) - \hat{\phi}_{in}(k)\sin\tilde{\phi}_{in}(k)\right] +$$

$$+ \sum_{\substack{m=1 \\ m\neq j}}^{N} \tau A_{jm} \left[\cos\tilde{\phi}_{jm}(k) - \hat{\phi}_{jm}(k)\sin\tilde{\phi}_{jm}(k)\right] + \bar{\zeta}_{ij}(k). \tag{11}$$

В (11) присутні усі складові рівняння, що і в (1). Тому віднімемо рівняння (1), попередньо представивши його в кінцево-різницевій формі, від рівняння (11).

Тоді для складових $\hat{\phi}_{ij}(k)$ справедливим буде таке співвідношення:

$$\hat{\phi}_{ij}(k+1)=\hat{\phi}_{ij}(k)-\sum_{\substack{n=1\\n\neq i}}^{N}\tau A_{in}\hat{\phi}_{in}(k)\sin\tilde{\phi}_{in}(k)-\sum_{\substack{m=1\\m\neq j}}^{N}\tau A_{jm}\hat{\phi}_{jm}(k)\sin\tilde{\phi}_{jm}(k)+\overline{\zeta}_{ij}(k). \qquad (12)$$

Вираз (12) є одним з рівнянь кінцевої різниці класичної системи стохастичних лінійних диференціальних рівнянь, що може бути зображено у векторній формі

$$\vec{\Phi}(k+1)=A(k)\vec{\Phi}(k)+\vec{\Xi}(k), \qquad (13)$$

де $A(k)=\left[a_{in}=\frac{\alpha_{in}}{2}\frac{A_n}{A_i}\sin\tilde{\phi}_{in}(k)\right]$ – фундаментальна перехідна матриця; $\vec{\Xi}(k)=\left[\overline{\zeta}_{in}(k)\right]$ – вектор адитивних шумів різниці фаз вихідних сигналів КМЧ.

Виходячи зі свого визначення, елементи a_{ij} матриці $A(k)$ складаються з добутку двох величин $\frac{\alpha_{in}}{2}\frac{A_n}{A_i}$ і $\sin\tilde{\phi}_{in}(k)$. Спосіб визначення першого співмножника викладено в [29]. Другий співмножник є тригонометричною функцією аргументу $\tilde{\phi}_{in}(k)$, що може бути виміряною прямими методами за допомогою частотного (фазового) компаратора. Проте, при цьому необхідно враховувати два фактори. По-перше, результат $y_{ij}(k)$ виміру компаратора має власні частотні і фазові шуми з коваріаційною матрицею R. По-друге, компаратор вимірює різницю фаз з точністю до деякої константи, що у цьому випадку є істотною, оскільки по суті визначає зрушення фази гармонійного співмножника елементів матриці $A(k)$.

З урахуванням зазначених факторів, стохастичний процес, що задовольняє рішенню рівняння (13), будемо розглядати як нестаціонарний випадковий марківський процес з перехідною матрицею, що змінюється у часі (від ітерації до ітерації). Ідентифікація стану еталона на основі рівняння (13) належить до класу некоректних задач математичної фізики, одержати рішення (оптимальної згладженої оцінки стану) якої можна шляхом застосування регуляризувальної процедури, що одержала узагальнену назву "лінійний фільтр Калмана". Для цього необхідно доповнити рівняння (13) рівнянням виміру з відомими параметрами.

Крім того, стосовно рівняння (13) необхідно знати: матрицю $A(k)$, початкове значення елементів $\hat{\phi}_{in,0}=\hat{\phi}_{in}(0)$ вектора $\vec{\hat{\Phi}}$, матрицю $R_{\Xi}(\tau)=M\left[\vec{\Xi}(t)\vec{\Xi}^{T}(t+\tau)\right]=Q\delta(\tau)$, коваріаційну матрицю шумів вимірювача R, початкове значення коваріаційної матриці $P(0)=M\left[\vec{\Psi}(0)\vec{\Psi}^{T}(0)\right]$, де $\vec{\Psi}(0)=\left[\hat{\psi}_i(0)\right]$ – вектор стохастичних складових фаз вихідних сигналів КМЧ при $k=0$.

Узагальнені амплітуди A_{in}, що входять до складу матриці $A(k)$, і початкові значення різниць фаз $\tilde{\phi}_{in,0}=\tilde{\phi}_{in}(0)$ можуть бути визначені за допомогою алгоритму, викладеному в [29].

Матриця $R_{\Xi}(\tau)$ являє собою діагональну матрицю. При цьому кожний діагональний елемент являє собою квадрат СКВ частоти відповідної міри, кількісне значення якого можна взяти з паспортних даних на КМЧ або з результатів останньої її повірки.

Як показує практика, застосування методу фільтра Калмана, значення вектора $\vec{\Psi}(0)$ й матриці $P(0)$ необхідні для ініціалізації процедури фільтрації й істотно впливають лише на

початковий етап оцінювання стану системи. У міру збільшення аргументу k (у стаціонарному режимі роботи фільтра) вплив похибок визначення початкових значень прагне до нуля. Зведення рекурентних співвідношень, які реалізують оцінку значень фаз вихідних сигналів КМЧ, що входять до складу групи, наведено в таблиці. Дані рекурентні співвідношення являють собою реалізацію методу фільтра Калмана, що належить до класу наближених алгоритмів фільтрації на основі локальної апроксимації "точного" рішення нелінійного рівняння стану.

Метод фільтра Калмана для вектора оцінок стану значень фаз сигналів КМЧ та КГВЧ

№ п/п	Послідовність дій
1	Початкові умови: $\vec{\tilde{\Phi}}(0,0)=0$; $\vec{\tilde{\tilde{\Phi}}}(0,0)=\left[\tilde{\phi}_{ij}(0)\right]$; $P(0,0)=Q$; $\vec{\tilde{\Psi}}(0)$=0.
2	Оцінка стану фаз КМЧ та КГВЧ: $\psi_i(k+1\|k)$ див. вираз (8) по отриманій оцінці $\phi_{ij}(k\|k)$ (див. п. 10).
3	Оцінка регулярної складової: $\vec{\tilde{\tilde{\Phi}}}(k\mid k-1)=F\left[\vec{\tilde{\tilde{\Phi}}}(k-1\mid k-1)\right]$, де $F[*]$ визначається рівнянням (4).
4	Оцінка вектора умовного середнього: $\vec{\tilde{\Phi}}(k\|k-1)=A(k-1)\vec{\tilde{\Phi}}(k-1\|k-1)$
5	Коваріаційна матриця умовного середнього: $P(k\|k-1)=A(k-1)P(k-1\|k-1)A(k-1)^T+Q$
6	Коефіцієнт підсилення: $K(k)=P(k\|k-1)\left[P(k\|k-1)+R\right]^{-1}$
7	Вектор нев'язок вимірів: $\vec{\upsilon}(k)=\vec{Y}(k)-\vec{\Phi}(k\|k-1)$
8	Оцінка стохастичної складової: $\vec{\tilde{\Phi}}(k\|k)=\vec{\tilde{\Phi}}(k-1\|k-1)+K(k)\vec{\upsilon}(k)$
9	Коваріаційна матриця: $P(k\|k)=[I-K(k)]P(k\|k-1)[I-K(k)]^T+K(k)RK(k)^T$
10	Оцінка повного вектора стану: $\vec{\Phi}(k\|k)=\vec{\tilde{\tilde{\Phi}}}(k\|k-1)+\vec{\tilde{\Phi}}(k\mid k)$

Результати моделювання ідентифікації вектора фаз вихідних сигналів групового еталону, що складається з двох КМЧ та КГВЧ, звірюваних між собою по повному графу звірень, на основі запропонованого методу, наведені на рис. 1. Штриховими лініями зображено поведінку фаз вихідних сигналів кожного КМЧ та КГВЧ, а безперервними лініями – відповідні фази після видалення з них результатів оцінок, отриманих за допомогою запропонованого методу. Безперервна лінія на рис. 1 визначає зсув в оцінках рішення вихідної системи рівнянь і по суті є похибкою лінеаризації вихідної нелінійної системи рівнянь.

Як показано в [29], критерієм наявності оптимальної незміщеної оцінки вектора стану $\vec{\Phi}(k\mid k)$ є рівність нулю величини $M[\vec{\upsilon}(k)]$.

На рис. 2 наведено поведінку елемента вектора нев'язок $\vec{\upsilon}(k)$ у часі. Видно, що його поточне значення еквівалентно поведінці центрованого випадкового процесу, що свідчить про відсутність зсуву в отриманих оцінках поточних значень фаз вихідних сигналів КМЧ та КГВЧ.

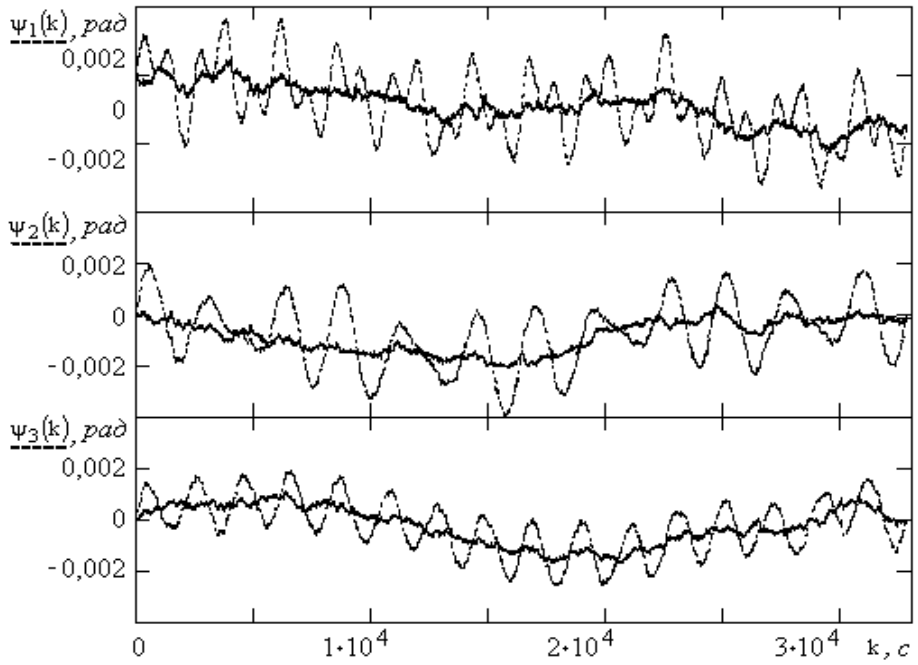

Рис. 1. Оцінка вектора фаз вихідних сигналів групового еталону, що складається з двох КМЧ та КГВЧ, звірюваних між собою по повному графу звірень

Проте, при застосуванні методу фільтра Калмана необхідно враховувати, що лінеаризація вихідної нелінійної системи рівнянь призводить до появи зсувів в оцінці рішення вихідної системи рівнянь. При цьому математичне очікування вектора нев'язок у фільтрі Калмана хоча й дорівнює нулю, але вектор нев'язок є кольоровим шумом. Цей факт може бути використаний у побудові адаптивних алгоритмів Калманівської фільтрації, що є проміжними між алгоритмами, заснованими на локальній апроксимації, і більш універсальними (але більш складними й громіздкими) алгоритмами, заснованими на інтегральній апроксимації.

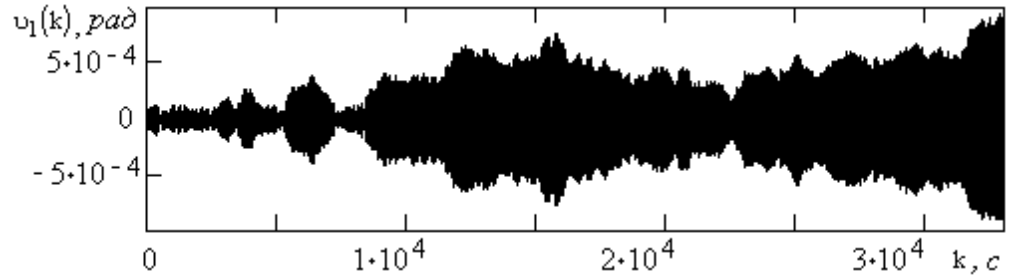

Рис. 2. Поведінка елементів вектора нев'язок у процесі ідентифікації системи стохастичної моделі системи пов'язаних осциляторів

Для розширення області існування оптимальних оцінок вектора стану $\vec{\Psi}(k)$ врахуємо ряд положень теорії оптимального керування [23]. Так, у теорії оптимального керування також доводиться мати справу з ідентифікацією систем за результатами вимірів і формуванням керуючих сигналів, пропорційних нев'язкам між оцінками умовного середнього й результатами вимірів.

Тому пропонується рівняння стану (6) доповнити складовою, що описує реакцію системи на уведене керування, тобто рівняння стану перепишемо у вигляді

$$\vec{\Psi}(k) = \Lambda(k, k-1)\vec{\Psi}(k-1) + B(k, k-1)\vec{U}(k) + \vec{\xi}(k), \qquad (14)$$

де $\vec{\Psi}(k)=[\psi_i(k)]$ – вектор стану (флуктуацій фази вихідних сигналів) КМЧ та КГВЧ; $\Lambda(k,k-1)$ – фундаментальна перехідна матриця; $B(k,k-1)$ – передатна матриця керування (виправлень); $\vec{U}(k)=[-\psi_i(k|k-1)]$ – вектор керування (виправлень); $\vec{\xi}(k)=[\xi_i(k)]$ – вектор адитивних шумів КМЧ та КГВЧ.

Порівнюючи (14) з (11), можна зробити висновок, що частину рівняння (11), яка описує поведінку різниць фаз вихідних сигналів мір частоти, може бути зображено як результат впливу керуючого сигналу $\vec{U}(k)$. В [22] показано, що фільтр Калмана дозволяє одержати оптимальну незміщену оцінку стану з мінімальною дисперсією тільки в тому випадку, якщо елементи матриць $\Lambda(k,k-1)$ і $B(k,k-1)$ задані коректно (оцінені правильно), а також показано, що при відхиленні оцінок елементів матриць $\Lambda(k,k-1)$ і $B(k,k-1)$ від оптимальних виявляються відхилення від оптимальності (зсув) у поведінці відновлень або нев'язок вимірів. Цей висновок є основним при розробці алгоритму ідентифікації системи, коли встановлюється й доводиться необхідна й достатня умова того, щоб помилки в елементах матриць $\Lambda(k,k-1)$ і $B(k,k-1)$ створювали зсув. Поширення даного положення на рівняння (11) дозволяє зробити твердження про те, що причиною виникнення зсувів у векторі нев'язок (вираз п. 7 у таблиці) є невірна оцінка передатної матриці $B(k,k-1)$ вектора керування. Дійсно, оцінки вектора керування, особливо відносно визначення дійсних значень різниць частот Δ_{ij}, можуть бути отримані як середнє на кінцевому інтервалі спостереження за системою й містити в собі як випадкові, так і систематичні складові похибок визначення.

Якщо матрицю $B(k,k-1)$ представити в діагональному виді, кожний діагональний елемент якої буде визначати відповідне середнє значення всіх різниць частот Δ_{ij}, то можна припустити, що обрана матриця неточно характеризує спостережувану систему, тобто точна матриця описується співвідношенням

$$\hat{B}(k,k-1)=B(k,k-1)-\delta B(k,k-1), \tag{15}$$

де $\hat{B}(k,k-1)$ – точне значення передатної матриці; $\delta B(k,k-1)$ – невідома похибка передатної матриці.

У цьому випадку дійсний стан системи (14) буде визначатися виразом

$$\vec{\Psi}_k=\Lambda(k,k-1)\vec{\Psi}_{k-1}+\hat{B}(k,k-1)\vec{U}_k+\vec{\xi}_k, \tag{16}$$

де $\vec{U}_k$ – точне значення вектора керування (виправлення) КМЧ та КГВЧ.

Оскільки матриця $B(k,k-1)$ задана не точно, у загальному випадку рівняння (15) стає неточним, тобто стають відмінними від нуля такі співвідношення, що описують умовне середнє:

$$\vec{m}(k\mid k)=M\left[\vec{\Psi}_k\right]-M\left[\vec{\Psi}(k\mid k)\right]; \tag{17}$$

$$\vec{m}(k\mid k-1)=M\left[\vec{\Psi}_k\right]-M\left[\vec{\Psi}(k\mid k-1)\right]. \tag{18}$$

Застосування операцій усереднення до рекурентних співвідношень фільтра Калмана з урахуванням (17), (18) дає такі зв'язки вектора середніх значень $\vec{m}(k\mid k)$, $\vec{m}(k\mid k-1)$ з матрицею помилок $\delta B(k,k-1)$:

$$\vec{m}(k\mid k)=[I-K(k)]\Lambda(k,k-1)\vec{m}(k-1\mid k-1)+[I-K(k)]\delta B(k,k-1)\vec{U}_k,$$

$$\vec{m}(k\mid k-1)=\Lambda(k,k-1)\vec{m}(k-1\mid k-1)-\delta B(k,k-1)\vec{U}_k.$$

В [22] показано, що існують граничні співвідношення:

$$\lim_{k\to\infty} M[\vec{\upsilon}(k)]\to\lim_{k\to\infty} M[\vec{m}(k\mid k-1)]=-[I-\Lambda(k,k-1)[I-K(k)]]^{-1}\delta B(k,k-1)\vec{U}_k.$$

Даний вираз являє собою функціонал, мінімізуючи який щодо елементів матриці $\delta B(k,k-1)$, можна одержати оцінки елементів даної матриці й тим самим мінімізувати похибку визначення вектора стану $\vec{\Psi}(k)$.

Вказане дозволяє записати рекурентну процедуру визначення елементів матриці $\delta B(k,k-1)$, яка органічно вписується в рекурентну процедуру фільтра Калмана (зведення розрахункових формул якого наведено в таблиці):

$$\frac{\partial \vec{m}(k\,|\,k)}{\partial \Delta_{ij}} = \left[I - K(k)\right]\left[\Lambda(k,k-1)\frac{\partial \vec{m}(k\,|\,k-1)}{\partial \Delta_{ij}} - \frac{\partial \delta B(k,k-1)}{\partial \Delta_{ij}}\right];$$

$$\frac{\partial \vec{m}(k+1\,|\,k)}{\partial \Delta_{ij}} = \Lambda(k,k-1)\frac{\partial \vec{m}(k\,|\,k)}{\partial \Delta_{ij}} - \frac{\partial \delta B(k,k-1)}{\partial \Delta_{ij}}.$$

Дані рівняння є стійкими різницевими рівняннями, тому вплив початкових умов згодом стає усе менш значним (ситуація, аналогічна з початковими умовами для фільтра Калмана). У зв'язку із цим, розглядаючи асимптотичну поведінку системи (принаймні поведінку системи після великої кількості вимірів), ці рівняння будемо вирішувати з початковою умовою $\frac{\partial m(k\,|\,k)}{\partial \Delta_{ij}} = 0$.

Внаслідок цього вирази (14) і (16) дозволяють враховувати похибку лінеаризації на основі визначення (уточнення) матриць $\Lambda(k,k-1)$ і $\delta B(k,k-1)$.

Через те, що оцінки знаходять шляхом проведення обчислювального експерименту на математичній моделі групового еталону, а не в результаті натурного експерименту, пропонуються такі заходи. Для реалізації локальної апроксимації «точного» рішення нелінійного рівняння стану в умовах проведення натурного експерименту необхідно використовувати оптимальний по збіжності й можливості апаратного керування (підстроювання частоти рубідієвої міри частоти полем «С») режим биттів. При цьому розведення частот вихідних сигналів КМЧ та КГВЧ у групі на інтервал, що перевершує смугу захвата частот, хоч і призводить до модуляції частоти вихідного сигналу кожної міри обмеженим набором квазігармонійних сигналів, проте дозволяє прогнозувати результуюче відхилення частоти й надалі компенсувати його. Внаслідок цього вдається одержати апріорну інформацію про тип рішення, одержати оцінки матриці коваріації похибки і вектора математичного очікування правої частини й рішення даної системи флуктуаційних рівнянь частоти (фази) коливань.

Принцип дії прототипу КГВЧ заснований на вимірюванні шумів вихідного сигналу КД на частоті електромагнітного поглинання при переході атомів рубідію з одного енергетичного стану в інший. Зовнішній вигляд експериментальної установки наведено на рис. 3. При виконанні робіт з дослідження квантових шумів КД виникла необхідність розробки плати IEEE 488 (керування), комутатора сигналів, компараторів (на рис. 3 частотомір Ч3-64/1 – 4 та цифровий осцилограф типу SDS1102CML – 5). Для одержання точного значення частоти переходу в атомах Rb87 вихідна напруга частотою 90 MHz у помножувачі прототипу КГВЧ (на рис. 3 прилад з приймачем сигналів GPS/GLONASS – 6) змішується з сигналом, що виробляється синтезатором А3 другої КМЧ типу СЧВ-74 (на рис. 3 прилад – 3). Варакторний діод КД одночасно виконує функції помножувача та змішувача, а резонатор КД (на рис. 3 прилад – 1), настроєний на частоту переходу, що дорівнює:

$$f_{0-0} = f_{vco} \cdot n_{mul} \cdot m_{mul} - f_{dds} \cdot k_m.$$

Тут f_{0-0} = 6834,682540 MHz, f_{vco} =5 MHz – частота керованого опорного генератору, n_{mul} =18 – коефіцієнт множення помножувача, m_{mul} =76 – коефіцієнт множення генератора гармонік, k_m =1, f_{dds} = 5,317460 MHz ± 4 kHz – частота цифрового синтезатора визначається

частотою 0-0 переходу Rb^{87} ячейки поглинання. Таким чином, змінюючи частоту синтезатора f_{dds}, можна з високою точністю налаштуватися на частоту збудження КД і, відповідно, виділити квантові фазові шуми.

Рис. 3. Зовнішній вигляд експериментальної установки (групового еталону), яка складається з двох КМЧ та прототипу КГВЧ

На схемі приймач сигналів GPS/GLONASS синхронізується сигналом опорної (першої) КМЧ частотою 5 MHz. Радіонавігаційні сигнали, прийняті антеною, надходять на антенний вхід приймача сигналів GPS/GLONASS, з виходу якого сигнал "1 PPS" (апаратна мітка часу) подається на вхід "Б" частотоміра типу Ч3-64/1. Секундна мітка від опорного (першого) генератора типу СЧВ-74 подається на вхід "А" частотоміра Ч3-64/1. При цьому частотомір працює в режимі виміру інтервалів часу. Інформація з виходу частотоміра Ч3 – 64/1 через інтерфейс IEEE488 передається в ПЕОМ для подальшої обробки й зберігання. ПЕОМ обладнана платою контролера інтерфейсу IEEE°488.

З виходу КД сигнал помилки надходить на осцилограф SDS1102CML та підсилювач низької частоти, з виходу якого посилений сигнал помилки подається на синхронний детектор модулятора КД та далі на блок синхронізації від другої КМЧ типу СЧВ-74 (на рис.°3 прилад°–°3). З виходу синхронного детектора напруга постійного струму надходить на інтегруючий підсилювач, що збільшує коефіцієнт регулювання опорного генератора КГВЧ системи імпульсного цифрового фазового автопідстроювання частоти без порушення її стійкості. Напруга з виходу інтегруючого підсилювача подається на керуючий елемент опорного генератора КД і впливає на нього так, щоб звести розстройку КД до нуля. Опорний генератор КГВЧ засинхронізований від першої КМЧ типу СЧВ-74 (на рис. °3 прилад°–°2).

Таким чином, частота опорного генератора КД в режимі автопідстройки буде дорівнювати $f_{vco} = (f_{0-0} + f_{dds} k_m)(n_{mul} m_{mul})^{-1}$.

У першому контурі автопідстроювання по частоті використовувалася перша КМЧ типу СЧВ-74. Рубідієві КМЧ типу СЧВ-74 мають нестабільність частоти вихідного сигналу за добу: $\leq \pm 1 \cdot 10^{-12}$. Замість КМЧ для частотної синхронізації КГВЧ можна використовувати метод загального охоплення для синхронізації опорного генератора КД по сигналам TV каналів [31]. При цьому для синхронізації опорного генератора КГВЧ сигналами 1 PPS по сигналам

TV каналів необхідно застосовувати також комплект апаратури GPS/GLONASS з похибкою у межах $\leq \pm 30$ ns. Це дозволить виключити похибку затримки радіотелевізійного передавального центру й мінімізувати похибку траси поширення.

Встановлено, що квантовий фазовий шум має гаусовський закон розподілу імовірності, тому для збільшення мінімальної ентропії та швидкодії необхідно використовувати методи та засоби збільшення ентропії. Тому в прототипі КГВЧ використовується спеціальний засіб збільшення ентропії – квантовий екстрактор [32].

Таким чином, запропонований метод вимірювання квантового фазового шуму та ширини лінії робочого переходу радіооптичної системи ГВЧ заснований на регуляризації задачі ідентифікації параметрів КГВЧ групою КМЧ за наявності похибки від взаємодії. Даний метод за результатами їх взаємних звірень дозволяє одержувати оцінки неспостережуваного процесу зміни поточних значень фази вихідного сигналу (вектора стану) КГВЧ та кожної КМЧ на основі апріорної інформації про групу як стохастичної системи зв'язаних осциляторів.

Висновки

Застосування методу ПРР в КГВЧ має великий потенціал для досягнення високої швидкості формування квантових дискретних випадкових послідовностей, достовірність яких може бути підтверджена метрологічним сертифікатом відповідності. На відміну від інших схем КГВЧ, даний метод дозволяє відпрацювати практичні схеми більшості методів генерації випадкових чисел. Тому запропонована перспективна схема високошвидкісного квантового ГВЧ заснована на вимірі випадкових коливань оптичного поля у ізотопах рубідію (Rb^{87}та Rb^{85}) КД. Запропонований метод вимірювання квантових флуктуацій фази спектрального джерела та ячейки поглинання має швидкодію порядку 1000 bit/s на один фотоприймач. Одним з важливих переваг цього підходу є високий потенціал швидкості генерації випадкових чисел (більш десятка Mbit/s) за рахунок використання матриці з фотодетекторів, яка може нараховувати декілька мільйонів одиниць фотодіодів.

Однак на даний час недостатньо вивчені квантові шуми інтенсивності радіооптичного резонансу при різних режимах оптичного накачування випромінюванням лампового спектрального джерела. Крім цього, основним зовнішнім чинником, що впливає на криптографічні параметри макету КГВЧ, є температура навколишнього середовища. Її вплив зводиться до температурного зрушення опорної частоти резонансу через недостатньо точний підбір складу суміші буферних газів в резонансних ячейках та затягуванням частоти СВЧ резонатором. Даний вплив на криптографічні параметри перспективного КГВЧ також вивчається.

Практична цінність роботи полягає у вирішенні питань, спрямованих на створення КГВЧ нового покоління, здатних поліпшити як свої криптографічні, так і масогабаритні характеристики за рахунок застосування в них різних джерел оптичного накачування парів рубідію. З застосуванням в КД напівпровідникових лазерів типу VCSEL, що випромінюють в діапазоні 780-900 nm, можуть бути створені достатньо прості джерела оптичного накачування для КГВЧ. Перспективним напрямком у побудові малогаборитних і швидкодіючих КГВЧ є використання фазового методу вимірювань в Λ-схемах з електромагнітно-індукованої прозорістю. Це дозволить значно зменшити масогабаритні характеристики прототипу КГВЧ.

Експериментальне підтвердження отриманих результатів проведено на прототипі КГВЧ з КД на парах рубідію Rb^{87}та Rb^{85}. Вихідні послідовності екстрактора перспективного КГВЧ успішно проходять статистичні тести DIEHARD і NIST STS.

Список літератури:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко // Харків : Форт, 2012. 878 с.

2. Гріненко Т.О. Квантові генератори випадкових чисел в криптографії / Т.О. Гріненко, О.П. Нарєжній // Системи обробки інформації : зб. наук. праць. Харків : ХУПС, 2015. Вип. 10(135). С. 86-89.

3. A Fast and Compact Quantum Random Number Generator/ Thomas Jennewien, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter and Anton Zeilinger 4/III D-80799 Munchen, Germany February 1, 2008. pp. 1–21. [Електронний ресурс] Режим доступу до матеріалів: https://arxiv.org/pdf/quant-ph/9912118.pdf.

4. U. Achleitner, Diploma Thesis, Innsbruck University (1997).
5. A. J. Martino, G. M. Morris, Applied Optics 30, 981 (1991).
6. G. M. Morris, Opt. Engin. 24, 86 (1985); J. Marron, A. J. Martino, G. M. Morris, Applied Optics 25, 26 (1986).
7. W. M. Itano, J. C. Bergquist, R. G. Hulet, and D. J. Wineland, Phys. Rev. Lett. 59, 2732 (1987).
8. Th. Sauter, W. Neuhauser, R. Blatt, and P. E. Toschek, Phys. Rev. Lett. 57, 1696 (1986).
9. Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum Random Number Generator using Photon-Number Path Entanglement. Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea-2013.
10. Kwon O., Cho Y.-W., Kim Y.-H. Quantum Random Number Generator using Photon-Number Path Entanglement // arXiv:0807.3440v2 [quant-ph] 4Aug 2008. pp. 1–4. [Електронний ресурс] Режим доступу: http://www.researchgate.net/publication/24218868.
11. Y.-H. Kim Phys. Rev. A 68, 013804 (2003).
12. Ritter T. // Cryptologia. Vol. 15, pp. 81 1991.
13. Stipčevića M., Medved Rogina B. Quantum random number generator based on photonic emission in semiconductors // Review of Scientific Instruments. Vol. 78 2007. pp. 1–7. [Електронний ресурс] Режим доступу: http://rsi.aip.org/rsi/copyright.jsp.
14. Stipčevića M. // Review of Scientific Instruments. Vol. 75 2004. pp. 4442.
15. Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng. Ultrafast quantum random number generation // Optics Express. 2012. Vol. 20. No. 11.
16. Qi B., Chi Y-M., Lo H-K., Qian L. Experimental demonstration of a high speed quantum random number generations cheme based on measuring phase noise of a single mode laser // Optics Letters. 2010. Vol. 35. pp. 312-314. [Електронний ресурс] Режим доступу: [arXiv:0908.3351v2 [quant-ph] 27 Aug 2009]: http://arxiv.org/abs/0908.3351.
17. V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Science 315, 966 (2007).
18. I. Goldbergand D. Wagner, Dr. Dobb's Journal, pp. 66-70 (1996).
19. ID Quantigue White Paper. Random number generation using quantum physics. Version 3.0, April 2010. http://www.idquantique.com.
20. Grinenko T. O., Narezhniy O.P., Gorbenko I.D. Methods for measuring the noise power spectral density of the random number generator quantum radio optical system // Telecommunications and Radio Engineering. 2017. Vol. 76. Issue 7. pp. 635-651. DOI: 10.1615/TelecomRadEng.v76.i7.60.
21. Стандарты частоты: принципы и приложения / Ф. Риле ; пер. с англ. Н. Н. Колачевского. Москва : Физматлит, 2009. 511 с.
22. Р.Ф. Оэп, А.Р. Стабберуд Фильтрация и стохастическое управление в динамических системах. Пер. с англ. ; под ред. К.Т. Леондеса. Москва : Мир, 1980. 408 с.
23. Л. Льюнг Идентификация систем. Теория для пользователя ; пер. с англ. ; под ред. Я.З. Цыпкина. Москва : Наука. Гл. ред. физ.-мат. лит., 1991. 432 с.
24. Чинков В.Н., Нарежний А.П. Математическая модель формирования групповой шкалы времени при условии взаимодействия атомных часов как системы связанных осцилляторов // Радіоелектронні і комп'ютерні системи. 2005. № 3(11). С. 5-9.
25. А.Ф. Верлань, В.С. Сизиков Интегральные уравнения: Методы, алгоритмы, программы. Справочное пособие. Киев: Наук. думка, 1986. 544 с.
26. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. Москва : Наука, 1974. 224 с.
27. Боголюбов Н.Н., Митропольский Ю.А. Асимптотические методы в теории нелинейных колебаний. Москва : Наука, 1974. 408 с.
28. Нарежний А.П. Идентификация скрытых периодичностей в нестационарных фазовых флуктуациях прецизионных мер частоты // Прикладная радиоэлектроника. 2005. Т.4. № 2. С. 148–152.
29. Евдокименко Ю.И., Нарежний А.П. Идентификация групповой меры частоты с использованием итерационных методов решения стационарных задач // Радиотехника. 1998. №109. С. 76–80.
30. Чинков В.Н, Нарежний А.П. Исследование режимов взаимодействия прецизионных мер частоты с близкими частотами // Авиационно-космическая техника и технология. 2005. №5(21). С. 52–56.
31. Гриненко Т.А. Устройство поддержки синхронизации по телевизионному сигналу для цифровой сети связи АСУ тп / Т.А. Гриненко, А.А. Костыря, А.П. Нарежний // Метрологія та прилади. 2014. №4. С. 44–50.
32. Нарєжній О.П. Метод побудови алгоритму екстрактора на основі багатомодульного перетворення для перспективного квантового генератора випадкових чисел / О.П. Нарєжній, Т.О. Гріненко // Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова НАНУ Кам'янець-Подільський : Кам'янець-Подільський нац. ун-т імені Івана Огієнка, 2017. Вип. 15. С. 126–132.

Харківський національний
університет радіоелектроніки;
Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 09.03.2018