УДК 623.61: 621.3.072.7

Лебідь Є.В. (НЦЗІ ВІТІ)
Шемендюк О.В. (НЦЗІ ВІТІ)
Чередниченко О.Ю. (НЦЗІ ВІТІ)
Штонда Р.М. (НЦЗІ ВІТІ)

ВБУДОВАНИЙ МОДУЛЬ ФАЗОВОГО АВТОПІДСТРОЮВАННЯ ЧАСТОТИ СХЕМИ ТАКТУВАННЯ ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

Дослідження робіт в галузі захисту інформації що обробляється в інформаційно-телекомунікаційних системах Збройних сил України, показали, що формування випадкових і псевдовипадкових послідовностей здійснюється за допомогою генератора випадкових чисел побудованих на базі мікроконтролерів, реалізованих на основі різних відомих методів. Проте через високий рівень внутрішніх шумів вбудованих підсилювачів мікроконтролера, на етапі відновлення тактового сигналу потрібно використовувати зовнішні широкосмугові прецизійні операційні підсилювачі, що призводить до збільшення розмірів, вартості та енергоспоживання генератора та робить його дуже вразливим до зовнішніх впливів.

У статті представлені принципи побудови схеми тактування мікроконтролера з вбудованим модулем системи фазового автопідстроювання частоти для тактування лінійного регістра зсуву зі зворотними зв'язками. Запропоновано новий варіант реалізації схеми тактування мікроконтролерів з вбудованим модулем системи фазового автопідстроювання частоти на основі модифікованого цифрового фазового детектора в залежності від заданих вимог рівня вихідного джитера системи. Проведено моделювання вбудованого модуля фазового автопідстроювання частоти за різних значень тактової частоти. Показано, що за результатами моделювання модуль системи фазового автопідстроювання частоти відповідає вимогам, які ставляться до систем тактування в мікроконтролерах загального призначення з погляду швидкодії та функціональних можливостей.

Висока швидкодія та стабільність роботи вбудованого модуля фазового автопідстроювання частоти в системах тактування робить генератор випадкових чисел у мікроконтролерах загального призначення перспективною платформою для широкого спектра пристроїв та систем, які потребують використання криптографічних операцій та протоколів.

Ключові слова: *генератори випадкових чисел, система ФАПЧ, фазовий джитер.*

Е. Лебедь, А. Шемендюк, А. Чередниченко, Р. Штонда. Встроенный модуль фазовой автоподстройки частоты схемы тактирования генератора случайных. *Исследование работ в области защиты информации обрабатываемой в информационно-телекоммуникационных системах Вооруженных сил Украины, показали, что формирование случайных и псевдослучайных последовательностей осуществляется с помощью генератора случайных чисел построенных на базе микроконтроллеров, реализованных на основе различных известных методов. Однако за высокого уровня внутренних шумов встроенных усилителей микроконтроллера на этапе восстановления тактового сигнала нужно использовать внешние широкополосные прецизионные операционные усилители, что приводит к увеличению размеров, стоимости и энергопотребления генератора и делает его очень уязвимым к внешним воздействиям.*

В статье представлены принципы построения схемы тактирования микроконтроллера со встроенным модулем системы фазовой автоподстройки частоты для тактирования линейного регистра сдвига с обратными связями. Предложен новый вариант реализации схемы тактирования микроконтроллеров со встроенным модулем системы фазовой автоподстройки частоты на основе модифицированного цифрового фазового детектора в зависимости от заданных требований уровня выходного джиттера системы. Проведено моделирование встроенного модуля фазовой автоподстройки частоты при различных значениях тактовой частоты. Показано, что по результатам моделирования модуль системы фазовой автоподстройки частоты соответствует требованиям, предъявляемым к системам тактирования в микроконтроллерах общего назначения с точки зрения быстродействия и функциональных возможностей.

Высокое быстродействие и стабильность работы встроенного модуля фазовой автоподстройки частоты в системах тактирования делает генератор случайных чисел в микроконтроллерах общего назначения перспективной платформой для широкого спектра устройств и систем, которые требуют использования криптографических операций и протоколов.

Ключевые слова: *генераторы случайных чисел, система ФАПЧ, фазовый джиттера.*

Y.Lebed, O.Shemendyk, O.Cherednichenko, R.Shtonda. Installed module phase auto adjustment the frequency scheme tasking the case generator. *Studies in the field of protection of information processed in information and telecommunication systems of the Armed Forces of Ukraine have shown that the formation of random and pseudorandom sequences is carried out by means of a random number generator built on the basis of microcontrollers, implemented on the basis of various known methods. However, due to the high level of internal noise of the microcontroller's built-in amplifiers, external wide-band precision operational amplifiers are required during the clock*

recovery phase, which increases the size, cost, and power consumption of the generator and makes it very vulnerable to external influences.

The principles of construction of the microcontroller clocking scheme with the built-in phase auto-frequency tuning module for clocking the linear shift register with feedback are presented in the article. A new variant of realization of the scheme of clocking of microcontrollers with the built-in module of system of phase autosadjustment of frequency on the basis of the modified digital phase detector depending on the set requirements of the level of the output jitter of the system is offered. The simulation of the built-in phase auto-tuning module at different clock frequencies is performed. The simulation results, the module of the phase auto-frequency tuning system meets the requirements that apply to clocking systems in general purpose microcontrollers in terms of performance and functionality.

The high speed and stability of the built-in phase auto-tuning module in clocking systems make the random number generator in general-purpose microcontrollers a promising platform for a wide range of devices and systems that require the use of cryptographic operations and protocols.

Key words: *random number generators, PLL system, phase jitter.*

Постановка завдання. У зв'язку з технічним прогресом є проблема захисту інформації,, що обробляється в інформаційно-телекомунікаційних системах Збройних сил України, від зовнішніх та внутрішніх загроз у кібернетичному просторі. Серед усього спектра методів захисту даних від небажаного доступу і збереження інформацією своїх основних властивостей особливе місце посідають криптографічні методи. При цьому намагаються досягти конфіденційності та цілісності інформації, що забезпечується такими криптографічними алгоритмами, як шифрування та хешування.

Важливою і невід'ємною складовою інформаційно-телекомунікаційних систем Збройних сил України, є вбудовані системи (ВС), де ціна та витрати енергії виходять на перший план, а обчислювальна потужність сконцентрована на високопродуктивних мікропроцесорах загального призначення у складі мікроконтролерів (МК) загального призначення [1, 2] . Основною проблемою вбудованих систем є те, що надзвичайно важко у готовому пристрої одночасно оптимізувати рівень безпеки, ціну та продуктивність. Як результат, існуючі криптоалгоритми доволі погано пристосовані до застосування у вбудованих системах, переважна більшість з яких ґрунтується на 8/16/32-бітових процесорах з малими обчислювальними ресурсами. Операції шифрування і хешування за традиційної програмної реалізації на МК загального призначення є доволі повільними і потребують значних витрат постійної і оперативної пам'яті. Генерація випадкових чисел на мікроконтролері, який є детермінованою системою, теж викликає відчутні складнощі – в результаті відомі ГВЧ є або повільними, або не достатньо випадковими. Відповідно пошук нових алгоритмів та способів реалізації, які б добре працювали на цих платформах, є важливим і актуальним завданням, з яким пов'язаний такий напрямок, як легковагова (lightweight) або малоресурсна криптографія.

Дослідження робіт в галузі захисту інформації показали, що формування випадкових і псевдовипадкових послідовностей (ПВП) здійснюється за допомогою відповідних генераторів (ГВЧ), реалізованих на основі різних відомих методів. Генератори випадкових чисел (ГВЧ) є важливими компонентами більшості криптографічних систем. Функції ГВЧ зводяться до генерації ключів у симетричних і асиметричних криптоалгоритмах, вироблення випадкових повідомлень у протоколів автентифікації, побудованих за схемою "запит-відповідь", формування бітів доповнення до потрібного розміру блока, утворення векторів ініціалізації у блокових шифрах та масок для протидії атакам через сторонні канали [1, 2]. Вразливість в алгоритмі роботи або реалізації ГВЧ може скомпрометувати всю криптосистему або значно послабити її криптостійкість, тому в криптографічних аплікаціях вимоги до якості ГВЧ найвищі.

Аналізуючи сучасний стан розвитку ГВЧ вбудованих системах, особливо на базі мікроконтролерів (МК), а також якості їх функціонування, стає зрозумілим, що потреба у створенні та розробці нових джерел генерації псевдовипадкових послідовностей, що поєднують у собі високу швидкодію і хороші статистичні властивості сформованої вихідної послідовності, досі залишається актуальною.

Отже, створення ефективного (щодо потрібних ресурсів, швидкодії та споживаної потужності) та якісного ГВЧ для вбудованих систем є непростим завданням.

Аналіз останніх досліджень і публікацій. Ідеальний ГВЧ здатний генерувати випадкові послідовності чисел, які статистично рівномірно розподілені, незалежні, непередбачувані та невідтворювані. Реальні ГВЧ, що використовуються в криптографії, лише певною мірою відповідають вказаним вимогам і відповідно до них поділяються на три базові класи [2]: генератори псевдовипадкових чисел (ГПВЧ), криптографічно-захищені ГПВЧ (КЗГПВЧ) та генератори істинно випадкових чисел (ГІВЧ).

ГПВЧ побудовані на певному детермінованому алгоритмі, який ініціалізується зовнішньозгенерованим випадковим числом – так званим зародком (seed). Відповідно, однакові значення зародка ГПВЧ завжди генерують однакові послідовності. Для забезпечення високого рівня захищеності ГПВЧ повинні періодично оновлювати значення зародка.

КЗГПВЧ ґрунтуються на ГПВЧ, але алгоритм, призначений для утворення випадкових чисел, унеможливлює в обчислювальному сенсі передбачення наступного значення, навіть якщо відомі сам алгоритм і попередні вихідні дані. З цією метою можуть використовуватися, наприклад, алгоритми гешування або симетричного шифрування.

ГІВЧ використовують або певний фізичний випадковий процес – тепловий шум, фазовий джитер, або певні випадкові явища – дії користувача, вміст ОЗП, сигнал від мікрофонного входу тощо. Оскільки ГІВЧ слугують для вироблення зародків у ГПВЧ та КЗГПВЧ, то можна стверджувати, що вони відіграють фундаментальну роль у захищеності всієї криптосистеми.

Для кожної задачі можуть бути прийняті до уваги окремі характеристики, які впливають на результат рішення задачі. Вони залежать від структури ГВЧ та алгоритму генерації бітової послідовності, а також значення має його програмна або апаратна реалізація.

У статті [3] описано типовий ГІВЧ, що використовує комбінацію аналогових і цифрових компонентів. Він складається з двох стабілітронів, які є джерелом білого шуму. Шумовий сигнал підсилюється до цифрових логічних рівнів та дискретизується за допомогою компаратора та тригера. Оскільки кола підсилення споживають достатньо багато потужності, мають аналоговий характер та вносять спотворення в сигнал, інтеграція подібних ГІВЧ у більшість мікроконтролерів чи FPGA проблематична.

В роботі [4] ГІВЧ пропонується побудувати на PSoC-мікроконтролері, який має розміщені на кристалі програмно конфігуровані аналогові кола (резистори, конденсатори, підсилювачі, компаратори). Проте, через високий рівень внутрішніх шумів вбудованих підсилювачів МК, на етапі відновлення тактового сигналу потрібно використовувати зовнішні широкосмугові прецизійні операційні підсилювачі. Крім збільшення розмірів, вартості та енергоспоживання генератора, це додатково робить його дуже вразливим до зовнішніх впливів.

ГІВЧ на основі цифрових генераторів використовують два незалежні генератори (без стабілізації частоти), відмінні внутрішні шуми яких спричиняють джитер фази (короткочасні зміщення фронтів у часі), що і є джерелом випадковості [2].

Недоліком такого методу є необхідність накопичення фази джитера впродовж тривалого часу (оскільки джитер цифрових генераторів достатньо малий), щоб отримати якісні випадкові дані, а це обмежує продуктивність ГІВЧ на рівні 1 Мбіт/с, що може бути недостатнім для високопродуктивних криптосистем.

Одним із варіантів до вдосконалення схеми незалежних генераторів полягає в їх використанні для тактування лінійного регістра зсуву зі зворотними зв’язками використовується окремий тактовий сигнал, який формується схемою тактування МК з спеціальним модулем системи ФАПЧ [5].

У технічній документації на мікроконтролери відсутня детальна кількісна оцінка якості вбудованого модуля системи ФАПЧ схеми тактування, а лише зазначено, що вони можуть

працювати з надвисокими тактовими частотами. Основною вимогою до модуля ФАПЧ є забезпечення низького рівня фазового джитера вихідного тактового сигналу.

Однак при дослідженні можливостей зниження фазового джитера вихідного сигналу системи фазового автопідстроювання частоти, була виявлена необхідність враховувати фазові шуми, що виникають у фазових детекторах, які використовуються в схемах фазового автопідстроювання частоти [6].

Таким чином, актуальними є проведення досліджень технічних рішень та методів компенсації рівня фазового джитера вихідного сигналу вбудованого модуля фазового автопідстроювання частоти в схемах тактування МК для побудови в генераторах випадкових чисел апаратури криптозахисту.

Метою роботи є підвищення ефективності мікроконтролерів загального призначення за рахунок фазового автопідстроювання частоти в системах тактування генераторів випадкових чисел в умовах фазового джитера.

Виклад основного матеріалу. Апаратний модуль ГІВЧ.

Розглянемо модуль RNG який є генератором випадкових чисел, що ґрунтується на безперервному аналоговому шумі. Апаратний модуль ГІВЧ побудований на джерелі аналогового шуму і забезпечує генерацію випадкових 32-бітних чисел.

Структурна схема апаратного модуля ГІВЧ наведена на рис. 1 [7].

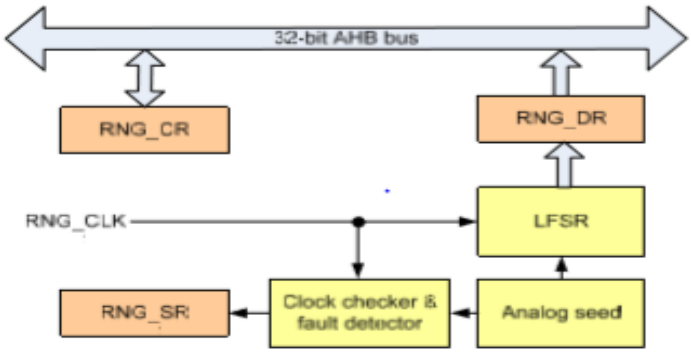

Рис. 1. Структурна схема модуля ГІВЧ

Аналогові кола генерують зародок, що надходить на лінійний регістр зсуву зі зворотними зв’язками (LFSR). Для тактування LFSR використовується окремий тактовий сигнал (RNG_CLK), який формується спеціальною схемою тактування (рис. 2).

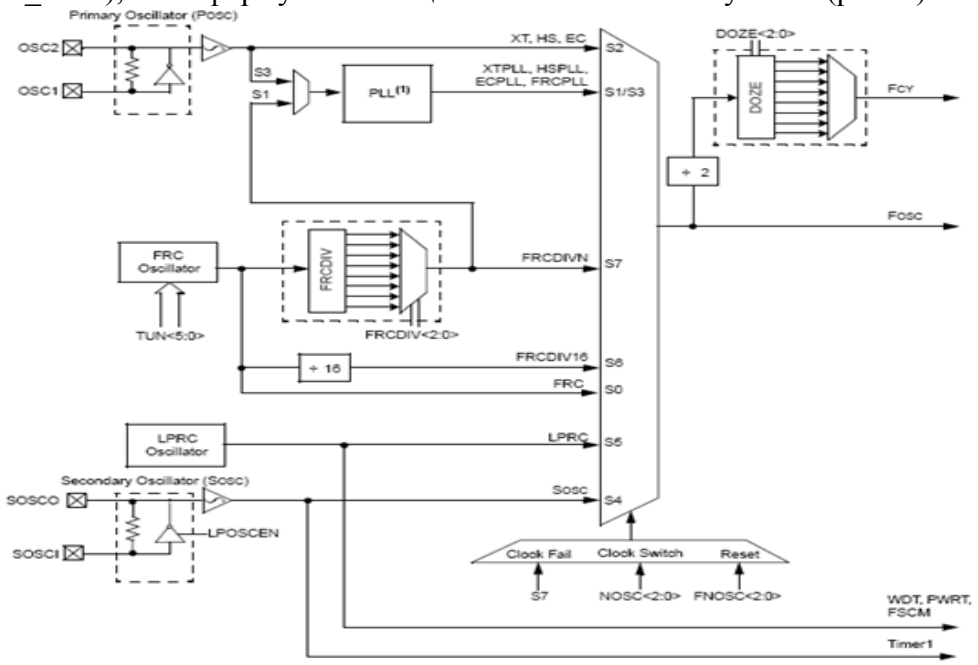

Рис. 2. Блок схема системи тактування

Система тактування забезпечує формування тактових сигналів для внутрішніх модулів МК та зовнішніх пристроїв. На виході схеми тактування безперервно формуються імпульси заданої частоти. Головними характеристиками генераторів є вихідна частота і стабільність частоти. Для отримання тактової частоти необхідно застосовувати внутрішні і зовнішні генератори тактової частоти (рис. 2).

Однак в роботі тактових генераторів існує проблема фазової неузгодженості тактових імпульсів. Для вирішення цієї проблеми необхідно вводити до складу мікроконтролерів спеціальний вбудований модуль ФАПЧ, який дозволяє покращити фазову неузгодженість тактових сигналів та підвищити швидкодію і функціональні характеристики окремих пристроїв.

В існуючих вбудованих модулях ФАПЧ спостерігається вплив фазового джитера за рахунок збільшення часу перехідних процесів, що призводить до зниження швидкості перестроювання за частотою, що, в свою чергу, призводить до зростання фазової помилки і, як наслідок, призводить до обмеження швидкості роботи МК.

Виходом із даної ситуації є застосування в системах ФАПЧ цифрових фазових детекторів з пристроєм оцінки неузгодженості сигналів [8].

Система ФАПЧ (рис. 3) є системою автоматичного регулювання, частота налаштування якої визначається частотою керуючого сигналу, а сигналом помилки є різниця фаз керуючого сигналу і сигналу зворотного зв’язку. На вхід системи подається керуючий сигнал, в якому фаза змінюється за випадковим законом з відомим розподілом. Фазовий детектор (ФД) визначає відставання або випередження вихідного сигналу відносно вхідного. Сигнали випередження чи відставання поступають на фільтр нижніх частот (ФНЧ). ФНЧ формує сигнали «додатній» чи «від’ємний» зсув, здійснюючи статистичну обробку сигналів «випередження» і «відставання».

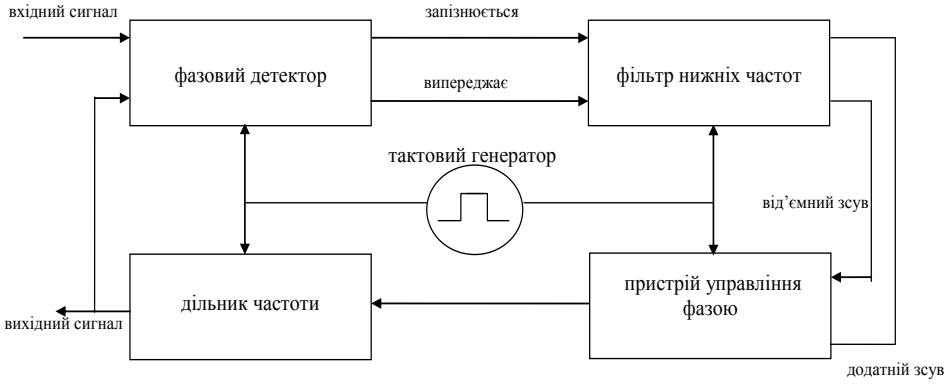

Рис. 3. Структурна схема системи ФАПЧ

У пристрої управління фазою, у разі появи сигналу «додатній зсув» до послідовності імпульсів, що виробляються опорним генератором (ОГ), додається один імпульс, у разі ж виникнення сигналу «від’ємний» зсув, з послідовності віднімається один імпульс. Далі перетворена послідовність імпульсів ділиться на ціле число L так, що вихідний сигнал дільника підстроєний за фазою з кроком підстроювання T_c чи $2\pi / L$. Таким чином, система ФАПЧ забезпечує рівність фаз вихідного і вхідного сигналів.

Значення фази вихідного сигналу, в цьому випадку, буде зсунуте відносно математичного очікування фази вхідного сигналу. Величина цього зсуву залежить від взаємного зсуву частот і фазового джитера вхідного сигналу. У випадку збільшення рівня підсилення в колі зворотного зв’язку, розширюється смуга захоплення, проте погіршується компенсація фазового джитера вхідного сигналу, що призводить до збільшення фазового джитера у спектрі вихідного сигналу системи ФАПЧ.

Основний недолік розглянутої вище структурної схеми системи ФАПЧ пов’язаний зі способом формування вихідної частоти. Для формування вихідної частоти необхідно мати

стабілізований генератор, вихідна частота, яка перевищувала б верхню границю необхідного діапазону вихідних частот системи ФАПЧ, що, в свою чергу, дозволить поєднати ширину полоси захоплення з можливістю компенсації фазового джитера.

В статті запропоновано метод компенсації фазового джитера вихідного сигналу системи ФАПЧ, який полягає в компенсації тренду фазового джитера вихідного сигналу системи, шляхом обчислення фазової помилки за модулем 2π, на основі модифікованого цифрового фазового детектора з пристроєм оцінки неузгодженості сигналів [7].

$$\varepsilon(\varphi) = K_{PD}\, sgn\left(\left|\Delta\varphi\right| mod\, 2\pi\right),$$

де $\varepsilon(\varphi)$ – сигнал помилки на виході ЦФД; K_{PD} – коефіцієнт передачі ЦФД; $\Delta\varphi = \varphi_{ref} - \varphi_{div}$ – фазова помилка на вході системи; $sgn(\cdot)$ – функція, яка повертає знак аргументу; $mod\, 2\pi$ – операція ділення за модулем 2π.

Обчислення фазової помилки за модулем 2π реалізовано шляхом формування на виході ЦФД цифрового коду помилки, який приймає значення з множини цілих чисел 0 ... N. Межі зміни коду від 0 (000 ... 0) до N (111 ... 1) у цьому випадку відповідатимуть зміни фазової помилки від -2π до 2π, код нульовий помилки N/2 (011 ... 1), а код помилки заноситься в пристрій оцінки сигналу неузгодженості.

Функціональна схема модифікованого ЦФД в якому реалізований даний підхід, показана на рис. 4. Модифікований ЦФД має два входи для сигналів f_{div} та f_{ref} і п’ять виходів: UP, DP – для фазової неузгодженості, UF, DF – для частотної неузгодженості і PHD – для виведення даних помилки на вихідну шину мікросхеми. Крім того, при переході з частотного режиму у фазовий і назад внутрішня структура детектора забезпечує перехід у стан, найбільш сприятливий з погляду завершення перехідних процесів, при переході в фазовий режим.

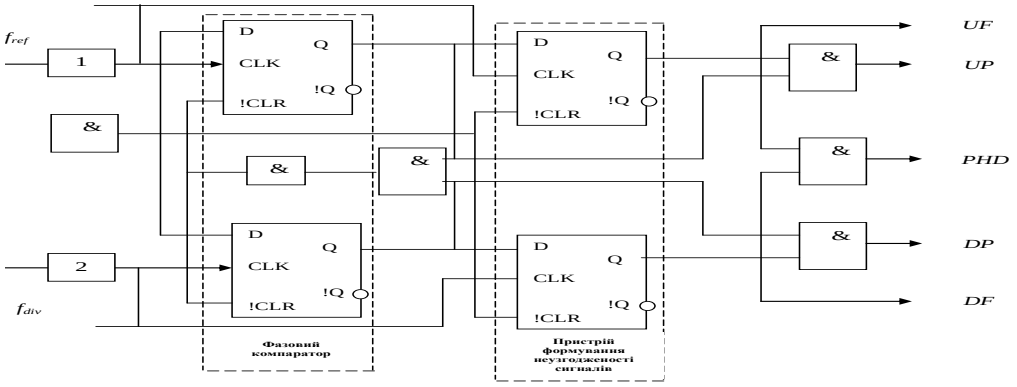

Рис. 4. Функціональна схема модифікованого ЦФД

На вхід ЦФД подається комплексний сигнал ОГ та синтезований сигнал ПГ. ЦФД вимірює фазову неузгодженість між двома сигналами. Далі сигнали поступають кожен на свій дільник частоти (ДЧ) з програмованими коефіцієнтами ділення K1 і K2, які задаються 9-розрядними кодами.

Потім сигнали надходять на тактові входи фазового компаратора (ФК), який здійснює порівняння поділених послідовностей, що поступають з виходів ДЧ. В результаті на виході ФК формується цифровий код шляхом підрахунку імпульсів ПГ за модулем N. По закінченню періоду сигналу, на виході ЦФД виникає імпульс скидання, який через пристрій затримки подається на входи CLR тригерів та встановлює їх виходи в початковий стан 011 ... 1, а код помилки заноситься в пристрій оцінки сигналу неузгодженості.

Якщо фазова помилка перевищує за модулем величину 2π, то в процесі перетворення виникає переповнення тригерів ФК, і вони переходять у початковий стан 011...1. У результаті, під час надходження чергового імпульсу з виходу ФК в пристрій оцінки сигналу неузгодженості заноситься код фазової помилки, взятої за модулем 2π. Якщо фаза сигналу з

виходу ОГ випереджає фазу сигналу ПГ, то на виході UP встановлюється стан логічної одиниці („лог. 1”), в іншому випадку стан логічного нуля («лог. 0»). Якщо різниця фаз обох сигналів не перевищує інтервал $\Delta\varphi_{min}$, то на виході UP встановлюється стан «лог. 0», а на виході PHD стан „лог. 1”.

Принцип роботи ЦФД, полягає в підрахунку числа тактів сигналу з виходу ПГ і порівнянні отриманого результату з відомим відношенням значення опорної частоти до необхідного значення частоти ПГ.

У режимі налаштування на частоту перетворення сигналу фазової помилки ЦФД в цифровий код здійснюється, як і в попередньому випадку, за допомогою ФК. Однак, при фазовій неузгодженості, що перевищує за модулем 2π, виходи UP, DP ЦФД блокуються, а на виходах UF, DF формується код помилки за частотою. Цифровий код з тригерів ФК через елемент затримки надходить на входи установки і скидання тригерів пристрою оцінки сигналу неузгодженості. У результаті тригери пристрою оцінки сигналу неузгодженості встановлюється в стан 0 (000 ... 0) або N (111 ... 1), у залежності від знаку помилки.

Код фазової помилки з виходів ЦФД надходить через ФНЧ на вхід ПГ. При цьому ФНЧ дозволяє формувати смугу пропускання контуру ФАПЧ у залежності від спектра інформаційного сигналу. Схема моделі модифікованого ЦФД відрізняється від існуючої моделі ЦФД в реалізації пристрою оцінки сигналу неузгодженості, що фіксує поточний стан детектора при фазовій помилці 2π і видає результат на вихідну шину мікросхеми.

Якщо значення сигналу неузгодженості лежить в інтервалі [–1; 1], то на виході PPD мікросхеми формується одиничне значення сигналу готовності ФД свідчить про те, що система ФАПЧ, налаштована.

Перехідні характеристики фазової помилки на виході модифікованого ЦФД представлено на рис. 5.

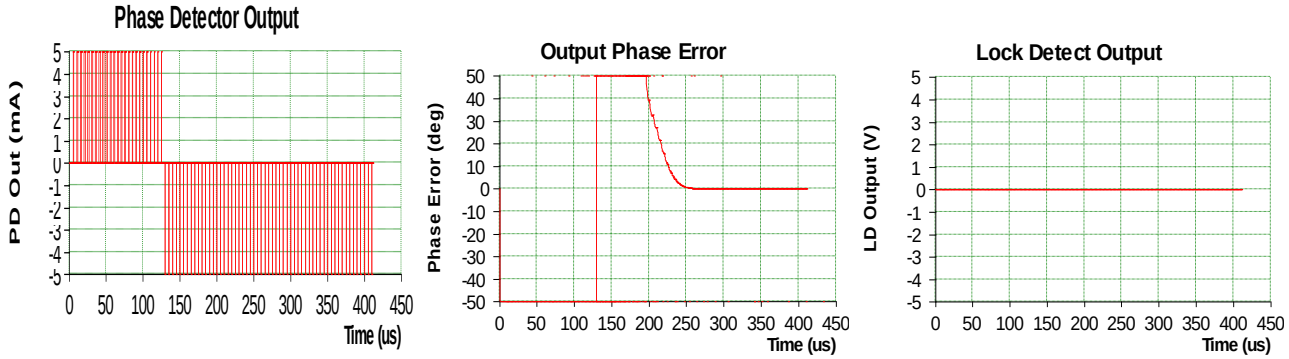

Рис. 5. Перехідні характеристики фазової помилки на виході модифікованого ЦФД

На рис. 6 представлені результати моделювання частотних характеристик системи ФАПЧ, за якими визначено запаси стійкості за фазою і амплітудою системи ФАПЧ з модифікованим фазовим детектором.

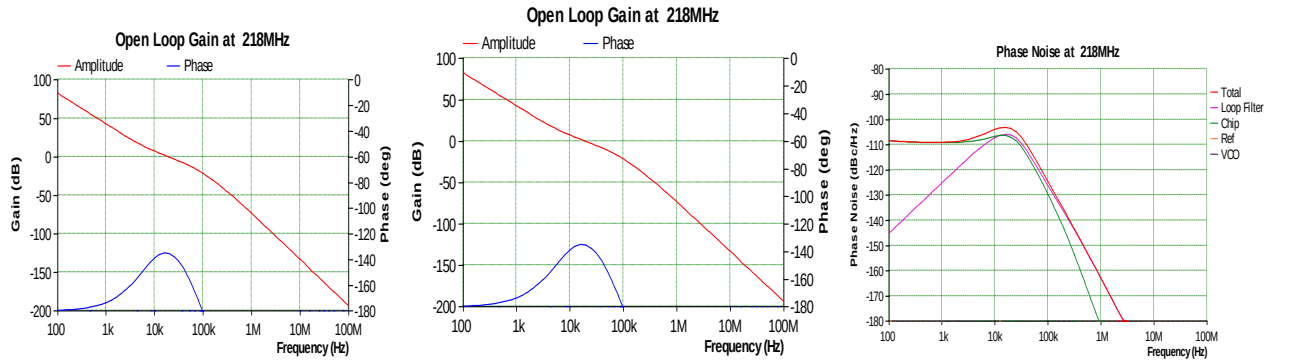

Рис. 6. Частотні характеристики системи ФАПЧ

На діаграмах (рис. 7) представлено результати моделювання перехідних процесів системи ФАПЧ.

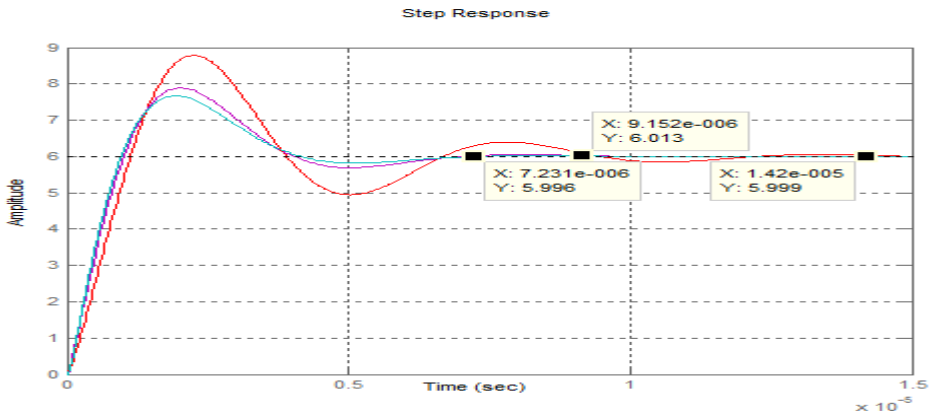

Рис. 7. Перехідні процеси системи ФАПЧ з модифікованим ЦФД

На рис. 8 представлені значення фазових шумів модуля ФАПЧ для різних значень частот. При низьких частотах (100 Гц – 1 кГц) фазовий шум на виході модуля змінюється в діапазоні –113…–155 дБн/Гц. На високих частотах (100 кГц – 1 МГц) фазовий шум залишається на одному рівні, в межах 160 дБн/Гц.

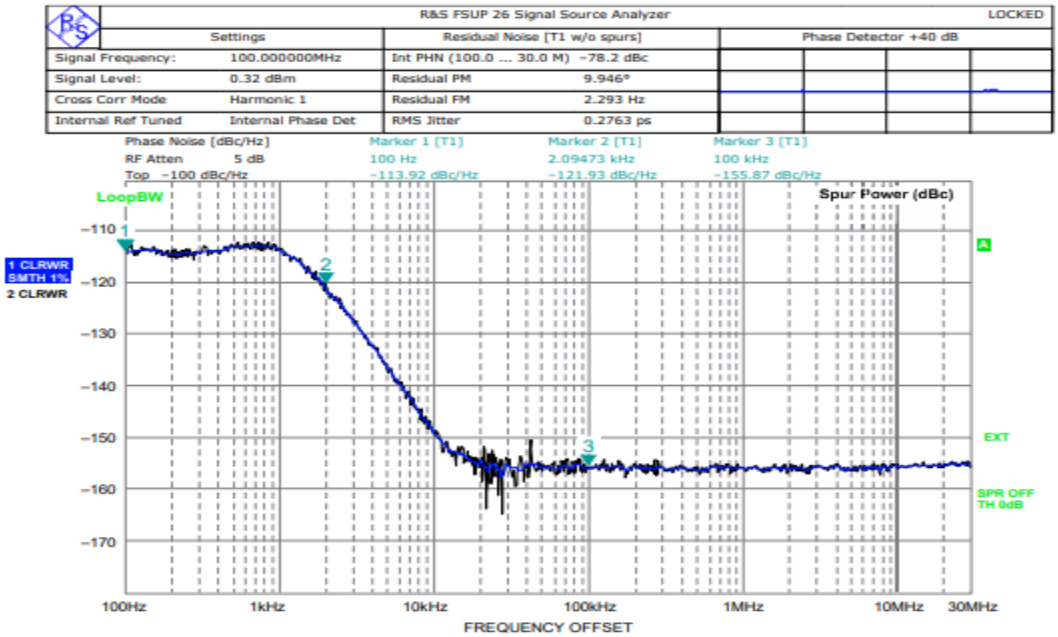

Рис. 8. Значення фазових шумів модуля ФАПЧ

Застосування модифікованого ЦФД дозволяє, залежно від поставлених завдань, компенсувати фазовий джитер системи ФАПЧ за критерієм мінімуму фазової неузгодженості. За рахунок введення модифікованого ЦФД можливо збільшити вхідну частоту, що, в свою чергу, призводить до швидкодії роботи МК.

Висновки

В даній статті розглянуто застосування модуля системи фазового автопідстроювання частоти в схемах системи тактування мікроконтролера генератора випадкових чисел.

В ході дослідження було вдосконалено модуль фазового автопідстроювання частоти схеми тактування генератора випадкових чисел, що дозволило компенсувати фазовий джитер вихідного сигналу системи до 7 %, у порівнянні з існуючою системою, шляхом введення модифікованого цифрового фазового детектора з пристроєм оцінки неузгодженості сигналу, який дозволяє підвищити динамічну точність системи в умовах фазового джитера до 11 %. За рахунок введення модифікованого ЦФД можливо збільшити вхідну частоту, що, в свою чергу, призводить до швидкодії роботи МК.

Висока швидкодія та стабільність роботи вбудованого модуля ФАПЧ в системах тактування робить ГІВЧ у мікроконтролерах загального призначення перспективною платформою для широкого спектра пристроїв та систем, в галузі телекомунікацій, вимірювань та захисту інформації.

Напрямками подальших досліджень є розробка методики чисельної оцінки параметрів вихідного тактового сигналу при підвищення фільтруючих можливостей вбудованого модуля системи фазового автопідстроювання частоти в схемах тактування мікроконтролерів в умовах фазового джитера.

ЛІТЕРАТУРА

1. Secure Integrated Circuits and Systems // Ed. Ingrid M.R. Verbauwhede. – Springer-Verlag, 2015. – 246 p. – ISBN 978-0-387-71827-9.

2. Cryptographic Engineering // Ed. Koc C.-K. – New York: Springer Science+Business Media, 2009. – 522 p. – ISBN 978-0-387-71816-3.

3. Killmann W., Schindler W. A Design for a Physical RNG with Robust Entropy Estimators // Proceedings of the 10th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'08), 2008, Washington, USA, LNCS, Vol. 5154, pp. 146-163, Springer, Heidelberg (2008).

4. Application Note AN2307. Consumer/Industrial Hardware Random Number Generator // Cypress Semiconductor, 2016, 12 p.

5. Шахгильдян В.В. Системы фазовой автоподстройки частоты / В.В. Шахгильдян, А.А.Ляховкин. – М.: Связь, 1972. – С. 1 – 220.

6. Kundert K.S., Predicting the Phase Noise and Jitter of PLL-Based Frequency Synthesizers. // Designer's Guide Consulting, Inc. Version 4f, November 2015. - www.designers-guide.org.

7. Совин Я. Р., Наконечний Ю. М, Стахів М. Ю. Дослідження характеристик вбудованого генератора випадкових чисел мікроконтролерів родини STM32F4XX згідно з методикою NIST STS // Вісник НУ „Львівська політехніка" „Автоматика, вимірювання та керування". – 2013. – № 753. – С. 37 – 44.

8. Лебідь Є.В. Метод компенсації фазових шумів системи фазового автопідстроювання частоти / Є.В. Лебідь, Шишацький А.В., Р.О. Бєляков // Науковий журнал „Телекомунікаційні та інформаційні технології", – 2017. – Київ: ДУТ. – № 2 (55). – С. 88 –97.

9. Іванов М., Чугункою И. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М., 2015.

10. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, May 2001, available at: http://csrc.nist.gov/rng/SP800-22b.pdf.

11. NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // National Institute of Standards and Technology Special Publication 80022 rev1a, 2014, 131 p.