УДК 681.3.07 (3.06)

Т.О. ГРІНЕНКО, канд. техн. наук, О.П. НАРЄЖНІЙ, канд. техн. наук,
І.Д. ГОРБЕНКО, д-р техн. наук

МЕТОДИКА ВИМІРЮВАННЯ СПЕКТРАЛЬНОЇ ЩІЛЬНОСТІ ПОТУЖНОСТІ ШУМУ КВАНТОВОЇ РАДІООПТИЧНОЇ СИСТЕМИ ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

Вступ

Важливими складовими криптографічних систем, від властивостей та характеристик яких залежить їх стійкість та криптоживучість та у цілому рівень безпеки критичних інформаційних технологій, є засоби управління ключами [1]. На різних етапах управління ключами необхідно генерувати ключові дані, ключову інформацію та різні параметри, до яких висуваються достатньо складні вимоги відносно властивостей. На практиці для генерації ключів, у залежності від вимог, застосовуються два методи – на основі випадкових та псевдовипадкових послідовностей, які реалізують у вигляді відповідних криптографічних засобів. В якості основних вимог до таких генераторів висуваються вимоги прямої та зворотної непередбачуваності (структурної скритності), необоротності відносно ключа, що використовується, нерозрізнюваності послідовностей, складності (швидкодії) та періоду повторення для псевдовипадкових послідовностей тощо [2].

При цьому рівень гарантій генераторів ключів суттєво залежить від ентропії джерела ключів, яка на сьогодні повинна складати від 128 до 512 бітів. Одним з таких джерел випадкових послідовностей є квантовий генератор випадкових чисел (КГВЧ). Як показали дослідження, такий генератор може задовольнити жорстким вимогам в частині необоротності, непередбачуваності, нерозрізнюваності та складності генерування. Тому аналіз та дослідження методів побудови високошвидкісних генераторів випадкових чисел (ГВЧ), заснованих на квантових процесах, обумовлює актуальність розробки вітчизняного високошвидкісного криптографічно стійкого КГВЧ.

Сучасна теорія припускає, що єдиний спосіб реалізувати чітке і зрозуміле фізичне джерело випадковості – це використання елементарних квантових рішень, так як в загальному розумінні виникнення кожного окремого результату такого квантово-механічного рішення об'єктивно випадкове. Існує ряд таких елементарних рішень, які є підходящими кандидатами для джерела випадковості. Найбільш очевидний – процес розпаду радіоактивного ядра (Kr^{85}, Co^{60}), який вже використовується [3]. Однак ці генератори є громіздкими, а використання радіоактивних матеріалів вимагає додаткових заходів обережності.

Альтернативою є оптичні процеси, які придатні для використання у якості джерел випадковості. До них відносяться: розщеплення окремих пучків фотонів, вимірювання поляризації одиночних фотонів, світло-темні періоди резонансного сигналу флуоресценції окремо захопленого іона [4 – 8]. Але тільки перші два з перелічених оптичних процесів досить швидкі і, крім того, не вимагають переважних технічних зусиль у їх реалізації.

Таким чином, на основі аналізу основних джерел [4 – 18] визначено, що в якості фізичних явищ при створенні КГВЧ використовують:

1. Дробовий шум – це шум в електричних ланцюгах, викликаний дискретністю носіїв електричного заряду, шум у оптичних пристроях. Як джерело шуму використовують фотоелектронний помножувач або електровакуумні фотоелементи;

2. Радіоактивний розпад, для якого характерна випадковість, забезпечується за допомогою кожного окремого акту розпаду. В результаті на приймач в різні проміжки часу потрапляє різна кількість частинок;

3. Квантовий оптичний процес як джерело випадковості.

При цьому, фізичні квантово-механічні ГВЧ на основі формування пучка фотонів з оптичними системами обробки є найбільш перспективними з точці зору використання в якості

генераторів випадкових послідовностей (ГВП). На сьогодні більшість КГВЧ засновано на виявленні одиночних фотонів, і найвищий досягнутий показник швидкості генератора випадкових чисел становить 16 Мбіт/с. Серед відомих генераторів даного типу за всіма критеріями кращим ГВЧ є квантовий генератор Quantis швейцарської компанії ID Quantique [19]. На відміну від відомих продуктів Quantis генерує випадкові числа з швидкістю передачі даних 4 – 16 Мбіт/с, це одна з найбільш високих швидкостей генерування випадкових чисел, підтверджена метрологічним сертифікатом відповідності. Даний КГВЧ сертифікований Швейцарським Федеральним Бюро Метрології (METAS), який відповідає за вимірювання у науці, тестування та відповідності. Також підтверджено, що вихідні послідовності КГВЧ Quantis успішно проходять статистичні тести DIEHARD і NIST (SP) 800-90A [20]. Сертифікати відповідності квантового ГВП Quantis представлено на сайті компанії ID Quantique [19].

На цей час розроблено досить велику кількість різних типів КГВЧ°[3-18]. Але для демонстрації їх статистичних властивостей використовувалися різні підходи до статистичного тестування [21]. Найчастіше набір і методику тестування пропонує сам розробник КГВЧ.

Таким чином, склалася ситуація, яка характеризується тим, що неможливо об’єктивно порівняти різні КГВЧ з єдиних позицій. Виходом з цього положення є використання деякого стандартного набору статистичних тестів, об’єднаних єдиною методикою розрахунку необхідних показників ефективності КГВЧ та прийняття рішення про випадковість формованих послідовностей.

Мета статті – обґрунтування вимог та розроблення методики дослідження властивостей КГВЧ, а також обґрунтування та вибір методів генерації випадкових послідовностей, які функціонують на основі квантових фізичних процесів. Метою досліджень було обґрунтування схеми високошвидкісного компаратора, що заснований на вимірі фазового шуму квантового дискримінатора (КД), який працює при відносно низькому рівні інтенсивності поблизу порогу генерації.

1. Основна частина

Фазовий шум є однією з найважливіших метрологічних характеристик КГВЧ як генератора шуму (ГШ) [22]. Відомо, що при визначенні фазових шумів вихідного сигналу досліджуваного ГШ застосовують два методи виміру – двогенераторний і тригенераторний [22 – 25]. Ці методи базуються на відсутності взаємного впливу (взаємодії) ГШ, що забезпечується апаратурним розв’язанням вимірювальних каналів у вимірювачі. При дослідженні (атестації) квантових ГШ необхідно одержати згладжену оцінку спектральної щільності потужності шумів (СЩПШ) фази („фонову” складову спектра) їх вихідного сигналу. Виходячи з цього, пропонується оцінку „фонової” складової здійснювати методами цифрової фільтрації за результатами вимірів фазових шумів у часі.

1.1. Математичне обґрунтування тесту спектральної щільності потужності шуму генератора випадкових чисел

Зв’язок між частотною й часовою областями задається у вигляді наступного лінійного інтегрального рівняння

$$\sigma^2(N,\tau)=\int_0^{\infty}\left|H(N,F,\tau)\right|^2\left|H_u(F)\right|^2 S_{\varphi}(F)dF\,, \qquad (1)$$

де $S_{\varphi}(F)$ – оцінка однобічної СЩПШ фази; $H_u(F)$ – частотна характеристика компаратора, еквівалентна фільтру нижніх частот зі смугою пропущення до частоти зрізу фільтра f_c; $H(N,F,\tau)$ – частотна характеристика цифрового фільтра, реалізованого при визначенні оцінки дисперсії $\sigma^2(N,\tau)$ для кількості вимірів в одній вибірці N й інтервалі часу виміру τ.

Для оцінки „фонової” складової спектральної щільності потужності ГШ по обмірюваних дисперсіях у часовій області необхідно вирішити зворотну задачу для інтегрального рівняння (1). Зворотна задача набагато складніше прямої, тому що поряд із проблемами збіжності виникають складності, пов’язані з її некоректністю [25]. Остання обставина при чисельних методах рішення виражається в поганій обумовленості систем лінійних алгебраїчних рівнянь, що вимагає застосування різних методів регуляризації [26, 27].

Викладені вище вимоги накладають обмеження на вид частотної характеристики $H(N,F,\tau)$ і, відповідно, на вибір виразів для одержання оцінок $\sigma^2(N,\tau)$. Найбільш раціональним для визначення „фонової” складової СЩПШ є використання двовибіркової дисперсії Алана, тому що вона є незміщеною, а кількість вимірів для одержання однієї оцінки мінімальна [25].

Таким чином, на підставі відомої [22 – 25] апріорної інформації про типи фазових шумів, що зустрічаються в ГШ, рівняння стану „фонової” частини СЩПШ із обліком (1) і за умови $\tau = T$ (T – інтервал часу між сусідніми вимірами) має вигляд

$$\sigma^2(2,\tau) = \frac{16 f_0^2}{\tau^2} \sum_{l=0}^{L=4} s_l \int_0^{\infty} \frac{\sin^4(\pi F \tau)}{F^l} |H_u(F)|^2 dF, \qquad (2)$$

де $\sigma^2(2,\tau)$ – дисперсія Алана ($N = 2$), отримана на інтервалі часу виміру τ; s_l – коефіцієнти розкладання СЩПШ у степінний ряд, що кількісно визначають різні види фазових шумів ГШ; f_0 – номінальне значення частоти опорного сигналу КГВЧ.

Урахуємо, що вхідні фільтри компаратора мають деяку граничну частоту пропущення f_c, усередині якої $|H_u(F)|$ є постійною величиною і різко убуває за межами смуги пропущення фільтра. Таким чином, без втрати точності рівняння (2) можна перетворити:

$$\sigma^2(2,\tau) = \frac{16 f_0^2}{\tau^2} \sum_{l=0}^{L=4} s_l \int_0^{f_c} \frac{\sin^4(\pi F \tau)}{F^l} dF. \qquad (3)$$

Процес виміру в часі оцінки дисперсії Алана (3) запишемо у вигляді

$$\left\langle \sigma^2(2,\tau_i,N_c) \right\rangle = \frac{1}{2(N_c-1)} \sum_{i=1}^{N_c-1} (z(\tau_{i+1}) - z(\tau_i))^2, \qquad (4)$$

де $z(\tau_{i+1})$ – результат виміру компаратором відносного відхилення фазових шумів $\bar{y}(\tau_{i+1}) = \frac{1}{\tau} \int_{t_i}^{t_i+\tau} y(t)dt$ досліджуваного ГШ від еталонної міри (ГШ) за інтервал часу виміру $(t_i, t_i+\tau)$; N_c – число вибірок; $\langle \varphi \rangle$ – середнє за часом випадкової величини φ.

З урахуванням (3) і (4) зв’язок між обмірюваними статистиками $\left\langle \sigma^2(2,\tau_i,N_c) \right\rangle$ й оцінками s_l коефіцієнтів розкладання „фонової” складової СЩПШ досліджуваного ГШ представимо у вигляді векторно-матричного рівняння стану:

$$\left\langle \vec{D}_A \right\rangle = G\vec{S} + \vec{\eta}, \qquad (5)$$

де $\left\langle \vec{D}_A \right\rangle = \left\langle \left[\sigma^2(2,\tau_i,N_c) \right] \right\rangle$ – вектор статистик дисперсії Алана, обмірюваних при різних характерних інтервалах часу виміру τ_i, розмірністю $V \times 1$ (V – параметр, що залежить від числа

вибірок і інтервалу часу спостереження); $\vec{S} = [s_l]$ – вектор коефіцієнтів розкладання спектральної щільності в степінний ряд розмірністю 5×1; $G = [g_{il}] = \int_0^{f_c} |\mathrm{H}_A(2, F, \tau_i)|^2 F^{2-l} dF$ – матриця вагових коефіцієнтів розмірністю $V \times 5$, ($\mathrm{H}_A(2, F, \tau_i)$ – частотна характеристика дисперсії Алана); $\vec{\eta} = [\eta(\tau_i)]$ – вектор розмірністю $V \times 1$, елемент якого визначають адитивні шуми, що виникають при вимірі статистик дисперсії $\sigma^2(2, \tau_i, N_c)$.

Похибка виміру $\eta(\tau_i)$, обумовлена обраним методом оцінки й шумами вимірів компаратора, має відомі перші моменти:

$$\left\langle \left[\eta(\tau_i) - m_\eta(\tau_i)\right] \cdot \left[\eta(\tau_j) - m_\eta(\tau_j)\right] \right\rangle = \sigma_\eta^2(\tau_i, \tau_j) = \sigma_\eta^2 \delta_{ij} \text{ і } m_\eta(\tau_i) = \langle \eta(\tau_i) \rangle,$$

де δ_{ij} – символ Кронекера.

Результат регуляризації обігу інтегрального рівняння (3) з урахуванням вектора оцінок (5) зваженим методом найменших квадратів представимо як

$$\vec{S} = \left[G^T \Sigma^{-1} G\right]^{-1} G^T \Sigma^{-1} \left\langle \vec{D}_A \right\rangle + \Delta\vec{S}, \tag{6}$$

де $\Sigma = \left[\sigma_\eta^2 \delta_{ij}\right]$ – коваріаційна матриця адитивних шумів компаратора, що виникають при вимірі статистик $\left\langle \sigma^2(2, \tau_i, N_c) \right\rangle$, розмірністю $V \times V$.

Зсув оцінки вектора коефіцієнтів розкладання спектральної щільності в степінний ряд $\vec{S}$, одержуваний з (6), визначається співвідношенням

$$\Delta\vec{S} = \left[G^T \Sigma^{-1} G\right]^{-1} G^T \Sigma^{-1} \vec{m}_\eta$$

і може бути врахований при відомому векторі $\vec{m}_\eta = \left[m_\eta(\tau_i)\right]$ розмірністю $V \times 1$, елементи якого є математичним очікуванням адитивних шумів виміру.

Розрахункові значення елементів матриці вагових коефіцієнтів G для різних видів фазових шумів наведено на рис. 1; вагові коефіцієнти відповідають: *а* – за частотні шуми типу випадкових блукань ($l = 4$); *б* – за частотний флікер шум ($l = 3$); *в* – за білий частотний шум ($l = 2$); *г* – за фазовий флікер шум ($l = 1$); *д* – за фазові шуми типу білого шуму ($l = 0$).

Для одержання значимих оцінок коефіцієнтів s_l характерні часи вимірів τ_i вибирають таким чином, щоб значення $1/\tau_i$ перекривали діапазони частот, на яких внески всіх членів „фонової” складової СЩПШ є вагомими.

Вірогідність і працездатність пропонованого підходу до згладжування оцінки СЩПШ підтверджується результатами натурних експериментів над прототипом квантового ГШ на парах Rb^{87}. В даному КД використовується спектрально-селективне накачування, де джерелом світла накачування служить газорозрядна лампа з парами Rb^{87}. Її світ пропускається через ячейку з парами Rb^{87}, які селективно поглинають довгохвильову складову надтонкої структури резонансної лінії.

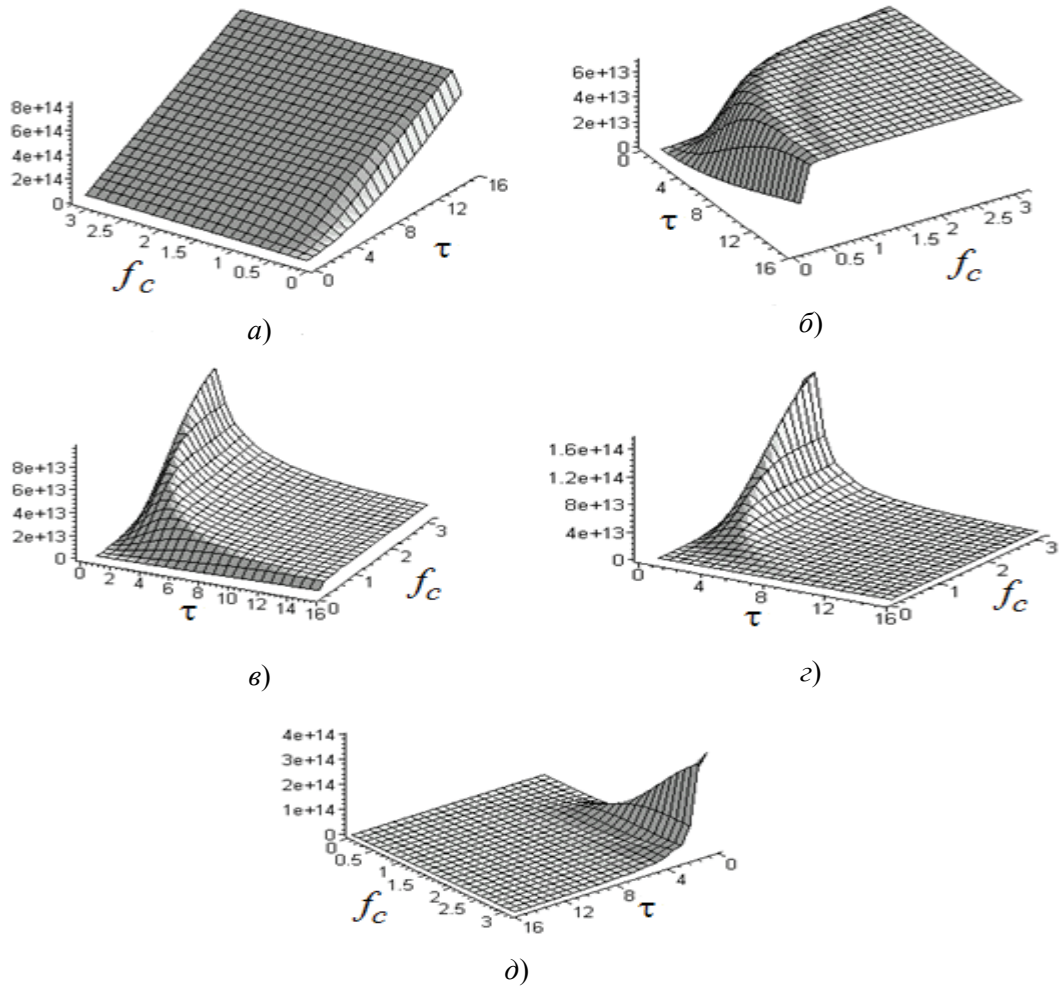

Рис. 1

Для того щоб придушити люмінесценцію оптичного фільтру (містить довгохвильову лінію), в фільтр додається молекулярний газ азот. В якості джерела накачування пропонується використовувати Vertical-Cavity Surface Emitting Laser (VCSEL), який характеризується досить симетричним просторово-кутовим розподілом вихідного пучка. Сучасні VCSEL також характеризуються великою межмодовою відстанню, що дозволяє гарантувати відсутність характерних для звичайних лазерів межмодових стрибків.

1.2. Апріорна оцінка похибки компаратора фазових шумів генератора випадкових чисел

Розгляд проведемо для випадку використання в якості фотодетектора КД напівпровідникового фотодіода з лавинним помноженням фотоструму. Отримані для цього випадку вирази легко поширити і на випадок безлавинного фотодіода. Основними складовими шумів на резисторі навантаження фотодетектора $R_н$ будуть:

1) Шуми, обумовлені струмами витоку фотодіода (і, в першу чергу, його темновим струмом), спектральна щільність напруги (струму) цих шумів наводиться підприємством-виготовлювачем в паспорті на фотодіод.

2) Фотонні (дробові) шуми потоку оптичного випромінювання (квантові шуми інтенсивності), обумовлені випадковими флуктуаціями кількості фотонів у потоці випромінювання, що є наслідком його енергетичної дискретності. Спектральна щільність даного шуму в широкому діапазоні частот постійна і належить білому гауссовському шуму [22 – 24]. Дисперсія напруги фотонних шумів (квантовий шум інтенсивності) $\sigma^2_{PD}(U_n)$ на резисторі навантаження $R_н$

$$\sigma_{PD}^2(U_n) = \frac{2e^2 P_{on}\eta_{PD}}{E_{ou}} M^2 F(M) R_н^2,$$

де e − заряд електрона, [Кл]; P_{on} − потужність оптичного потоку на вході фотодетектора КД, [Вт]; η_{PD} − квантова ефективність фотодетектора; $E_{ou} = h\nu$ − енергія кванта оптичного випромінювання [Дж], а $h \approx 6.62 \cdot 10^{-34}$ − постійна Планка [Дж×с] і ν − частота оптичного накачування КД [Гц]; M^2 − середній квадрат коефіцієнта лавинного множення (для лавинного фотодіода фотодетектора КД); $F(M)$ − чинник, що враховує додатковий шум із-за неідеальності процесів множення лавинного фотодіода (у разі використання не лавинних фотодіодів величини M^2 і $F(M)$ дорівнюють одиниці).

3) Дисперсія теплового шуму самого резистору $R_н$ (шум Найквіста):

$$\sigma_T^2(U_n) = 4k_B T_K R_н,$$

де k_B – постійна Больцмана ($k_B \approx 1.38 \cdot 10^{-23}$ Вт/град·Гц); T_K – температура навколишнього середовища в градусах Кельвіна.

4) Дисперсія власних шумів напруги $\sigma_{Al,\varphi}^2(U_n)$ вимірювача (компаратора) визначається як дисперсія Алана $\sigma_{Al,\varphi}^2$ приведена до смуги 0,5 Гц.

Структурна схема компаратора для вимірювання фазових шумів КГВЧ згідно з відомим алгоритмом вимірювання “дельта-квадрат” наведена на рис. 2. Компаратор фазових шумів КД складається з двох основних блоків: аналогового (Comparator (A)) і цифрового (Comparator (D)) однобітного аналого-цифрового перетворювача (ADC). На рис. 2 входи компаратора позначені: "SPD" – сигнал фотодетектора КД (Single Photon Detector); "RF QRNG" – еталонне значення частоти модуляції КД (Reference Frequency Quantum Random Number Generator); "RF" – сигнал опорної частоти КГВЧ. Точність вимірювання фазових шумів КД за допомогою даного компаратора обмежується двома основними видами похибок, а саме, шумами аналогово блоку і похибкою дискретизації цифрового блоку.

Похибка дискретизації вимірювань фазових шумів $\Delta\nu$ компаратора визначається частотою проходження калібрувальних імпульсів компаратора (100 МГц) і в кількісному відношенні визначається виразом

$$\Delta\nu = \frac{\min\{\Delta f_X\}_{\Delta t}}{f_0} \approx \frac{f_X^r}{f_{0n}\Delta t f_0},$$

де f_{0n} − частота калібрувальних імпульсів (~ 100 МГц); f_X^r − різницева частота досліджуваного сигналу (~ "RF QRNG" Гц); Δt – інтервал часу усереднення.

Похибка $\Delta\nu$ є випадковою величиною, рівномірно розподіленою на інтервалі $\left(-\frac{f_X^r}{f_{0n}\Delta t f_0}; +\frac{f_X^r}{f_{0n}\Delta t f_0}\right)$ з математичним очікуванням $\langle\Delta\nu\rangle = 0$.

Дисперсія похибки квантування визначається виразом

$$\sigma_{\Delta\nu}^2 = \int_{-\infty}^{\infty} (\Delta\nu)^2 p(\Delta\nu)\partial(\Delta\nu) = \frac{1}{3}\left(\frac{f_X^r}{f_{0n}\Delta t f_0}\right)^2,$$

де $p(\Delta\nu)=\begin{cases}\dfrac{f_{0n}\Delta t f_0}{2f_X^r}, & \text{при} \quad -\dfrac{f_X^r}{f_{0n}\Delta t f_0}\le\Delta\nu\le\dfrac{f_X^r}{f_{0n}\Delta t f_0};\\ 0, & \text{при} \quad \Delta\nu\le-\dfrac{f_X^r}{f_{0n}\Delta t f_0} \text{ и } \Delta\nu\ge\dfrac{f_X^r}{f_{0n}\Delta t f_0}.\end{cases}$

Розглянемо вплив похибки дискретизації на розрахункові значення дисперсії Алана і дисперсії Адамара, які є основними характеристиками квантових шумів у часовій області. При цьому будемо вважати, що флуктуації частоти дорівнюють нулю, тобто $\left\langle f_X^r \right\rangle = f_X$.

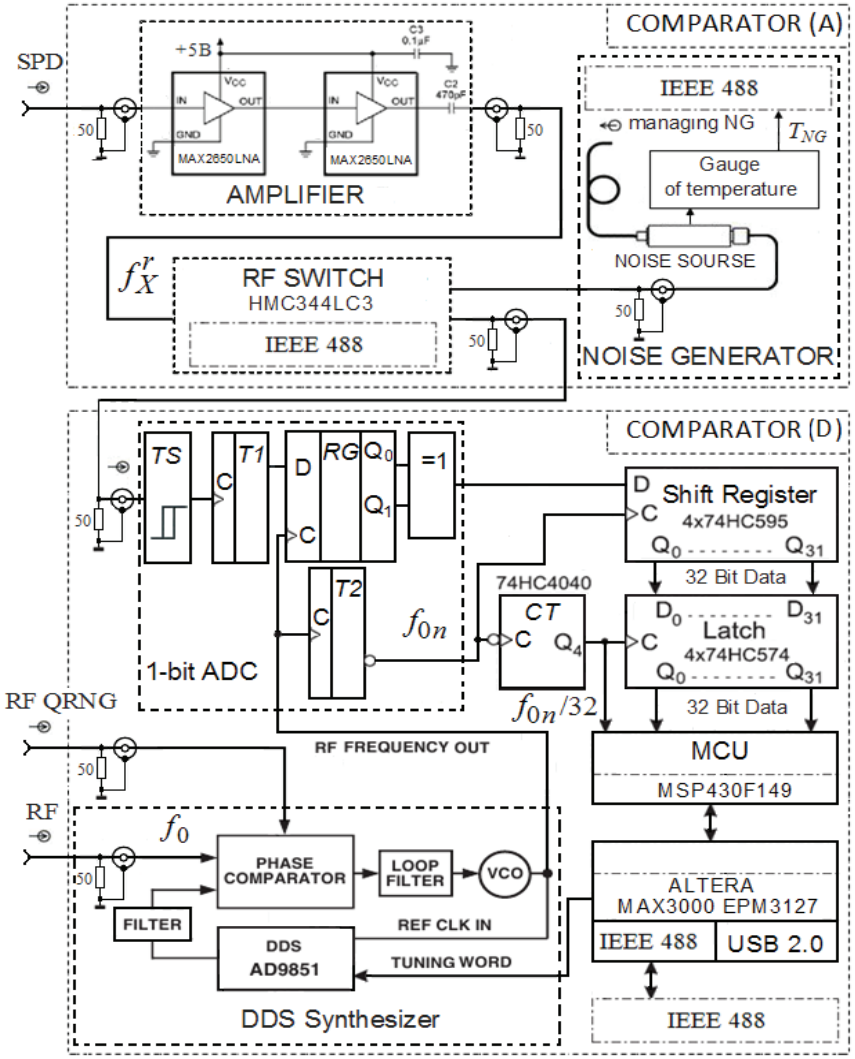

Рис. 2

Дисперсія Адамара визначається на підставі такого непрямого виміру:

$$L_A=\sum_{i=0}^{2m-1}(-1)^i\,\bar{y}_i,$$

де $\bar{y}_i=\dfrac{\Delta\varphi_X(t_i+\Delta t)-\Delta\varphi_X(t_i)}{2\pi f_0\Delta t}$, $\Delta\varphi_X$ – виміряна різниця фаз між опорним "RF QRNG" і досліджуваним сигналом "SPD".

Відповідно до центральної граничної теореми L_A – рівномірно розподілена випадкова величина з математичним очікуванням $\langle L_A \rangle = 0$. У цьому випадку дисперсія величини L_A буде дорівнювати

$$\left\langle \left(L_A - \langle L_A \rangle\right)^2 \right\rangle = \sum_{i=0}^{2m-1} \sum_{j=0}^{2m-1} (-1)^i (-1)^j \left\langle \bar{y}_i \bar{y}_j \right\rangle .$$

При незалежних вимірюваннях відхилення частоти від номінального значення $\bar{y}_j$ кореляційна функція $K = \left\langle \bar{y}_i \bar{y}_j \right\rangle$ при $i \neq j$ дорівнює нулю. Оскільки величина $\bar{y}_j$ – центрована, то для дисперсії випадкової величини L_A будемо мати

$$\left\langle L_A^2 \right\rangle = \frac{2m}{3} \left(\frac{f_X^r}{f_{0n} \Delta t f_0} \right)^2 .$$

При $m = 1$ даний вираз дає оцінку дисперсії Алана для шумів квантування при вимірюванні відхилення частоти входів "RF QRNG" і "SPD" в режими калібрування

$$\sigma_{Al,f}^2 = \frac{2}{3} \left(\frac{f_X^r}{f_{0n} \Delta t f_0} \right)^2 .$$

Оцінка дисперсії Алана шумів квантування при вимірюванні фазових шумів КГВЧ, віднесених до номінального значення частоти f_0, відповідно

$$\sigma_{Al,\varphi}^2 = \frac{2}{3} \left(\frac{f_X^r}{f_{0n} f_0} \right)^2 .$$

Сумарну похибку вимірювання фазових шумів, внесену компаратором, можна оцінити шляхом його калібрування. З цією метою на обидва входи "RF QRNG" і "SPD" подається сигнал від одного джерела. Компаратор встановлюється в режим вимірювання "U_N". Виробляються суміжні вибірки з N слідуючих друг за другом вимірювань фазових шумів при всіх інтервалах усереднення. За даними вибірками проводиться оцінка дисперсій сумарної похибки $\sigma_{Al,f}^2$ для різних інтервалів часу усереднення:

$$\sigma_{Al,f}^2 = \sqrt{\frac{1}{N-2} \sum_{i=2}^{N} \left((z_i - 2z_{i-1} + z_{i-2}) / \Delta t \right)^2} ,$$

де z_i – дані вимірювань, що видаються компаратором на інтерфейс IEEE 488 (рис. 2).

На рис. 3 наведена гістограма розподілу ймовірностей після схеми отримання випадкових біт фотоструму з КД та її апроксимація нормальним законом розподілу виду $Hist_j \in N\left(0, \sigma_{\Delta z}^2\right)$.

Результати проведених оцінок дисперсії сумарної похибки компаратора (графік 1) та рівня шумів дискретизації (графік 2) в залежності від інтервалу усереднення Δt наведено на рис. 4. Там же наведено оцінки дисперсії власних шумів вбудованого в синхронометр Ч7-17 (графік 4) опорного кварцового генератору і квантового стандарту частоти Ч1-74 (графік 3).

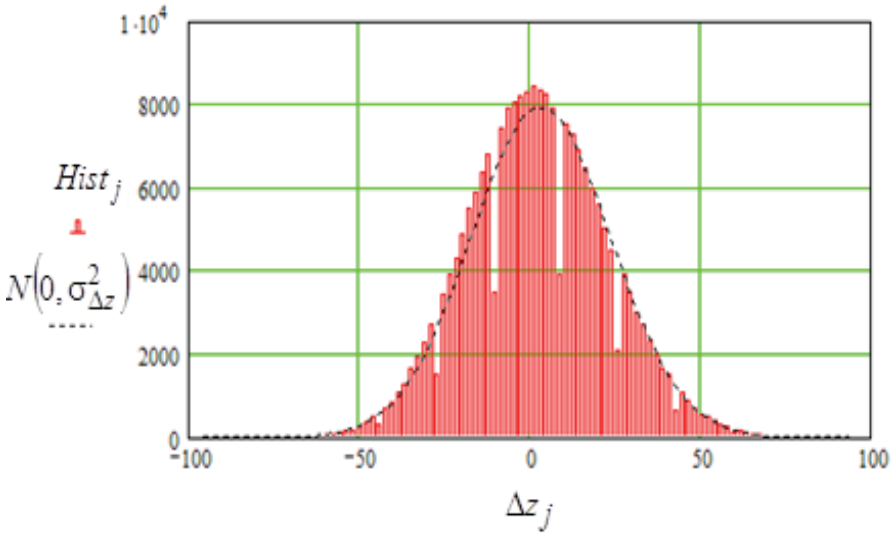

Рис. 3

Слід зазначити, що при розбіжності передніх фронтів імпульсів в компараторі не відбувається повної компенсації шумів синтезатора. Зменшення впливу зазначеного фактора можливо шляхом використання єдиного синтезатора для компаратора та КГВЧ, що дозволяє провести кореляційну обробку результатів вимірювань квантових шумів.

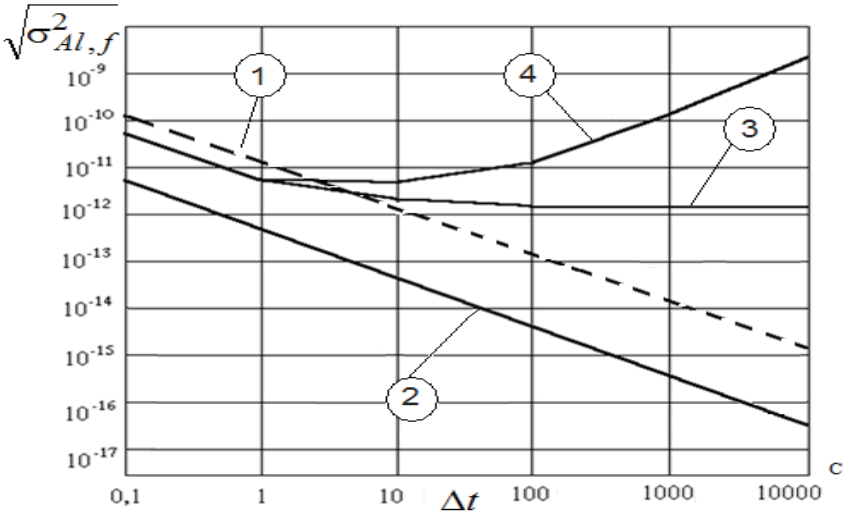

Рис. 4

Як правило, результати вимірювань можна подати у вигляді суми лінійних комбінацій компонент вектора стану КГВЧ і $\eta_{ком}$ – сумарного шуму компаратора. Тому апріорна оцінка коваріаційної матриці $M[\vec{\eta}_{ком}, \vec{\eta}^{T}_{ком}]$ дозволяє спростити алгоритми обробки результатів вимірювань квантових шумів.

Джерела цих шумів некорельовані між собою, тому сумарна похибка вимірювання фотонних (дробових) шумів потоку оптичного випромінювання (квантових шумів інтенсивності) визначається як

$$\sigma_{\Sigma}(U_n) = \sqrt{\sigma^2_{PD}(U_n) + \sigma^2_{T}(U_n) + \sigma^2_{Al,\varphi}(U_n)}\,.$$

Ця оцінка використовується для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, породжуваних КГВЧ.

1.3. Метрологічні характеристики квантових генераторів шумів

Відомо, що основні розрахункові співвідношення для оцінки метрологічних характеристик ГШ необхідно представляти в наступному вигляді:

1) Вираз для ENR (Excess Noise Ratio):

$$dB\ ENR = 10\log\left[\left(T_K / T_{NG}\right) - 1\right],$$

де T_{NG} – номінальна температура ГШ в градусах Кельвіна ($T_{NG} = 290K$).

2) Потужність шуму P_n в смузі частот B_f визначається виразом

$$P_n = k_B T_K B_f,$$

де B_f – смуга частот, Гц.

Результати вимірювань дисперсії Алана фазових шумів КД в залежності від інтервалів часу виміру τ_i наведено на рис. 5. На рис. 6 наведено СПЩШ з урахуванням порогу спрацьовування однобітного ADC компаратора, де графік: 1 – програмний ГВЧ, який реалізує алгоритм Блюм-Блюма-Шуба (англ. Algorithm Blum-Blum-Shub, BBS) [1]; 2 – апаратно-програмний ГВП, ключ електронний "Кристал-1", в основу якого покладений фізичний ГШ [2]; 3 – результати оцінки, що отримані за допомогою методики, яка викладена у роботі [25]; 4 – результат оцінки, отриманий згідно з запропонованою методикою.

На основі аналізу виду графіка 4, що наведений на рис. 6, спектральну щільність квантових ГШ можна поділити на дві категорії. На високих частотах домінує білий шум, а на низьких – флікер-шум (1/F-шум). Для білого шуму характерна рівномірна спектральна щільність. У цьому випадку енергія сигналу буде однакова в будь-якій заданій смузі частот. У випадку флікер-шуму енергія сигналу буде однакова в кожній декаді. Частота, нижче якої інтенсивність флікер-шуму починає перевищувати інтенсивність білого шуму, називається частотою зламу F_C.

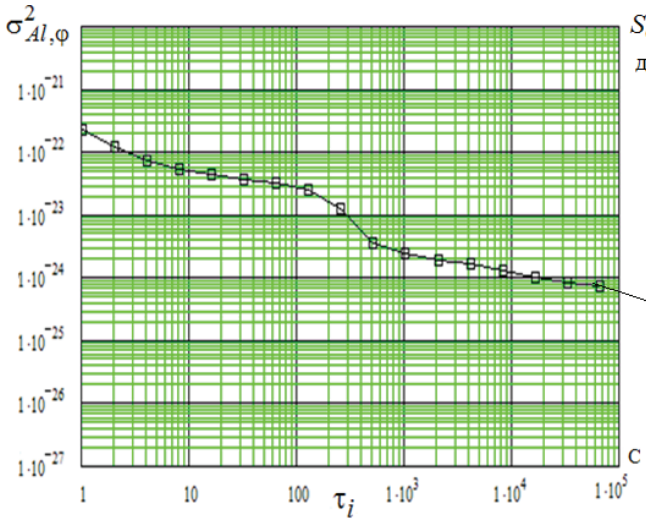

Рис. 5

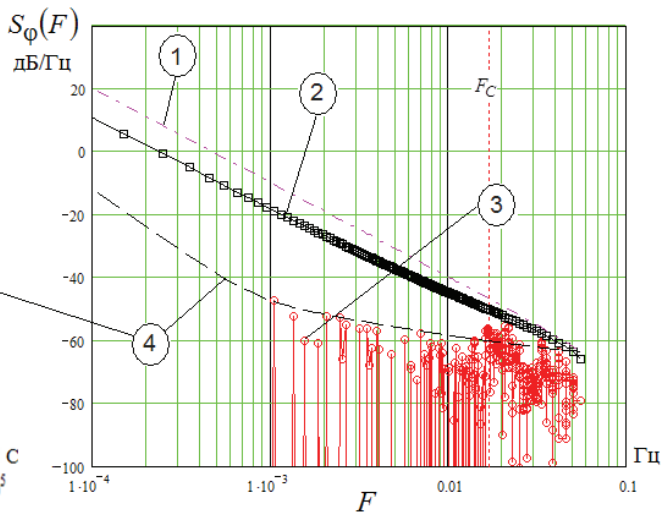

Рис. 6

Напругу шуму квантових ГШ в смузі частот можна оцінити, взявши спектральну щільність білого шуму $S_{ND}\left(B_f\right)$ з таблиці калібрувальних параметрів, верхню F_h і нижню F_l робочі частоти:

$$U_n = S_{ND}\left(F_h - F_l\right)\sqrt{F_h - F_l}\ \text{[В]}. \qquad (7)$$

У рівняння (7) не входить флікер-шум і, отже, воно вірно тільки для діапазонів, частота нижньої межі яких істотно більше частоти зламу ($F_l >> F_C$). Теоретично можна передбачити напругу шуму в будь-якій бажаній смузі частот, якщо спектральна щільність білого шуму $S_{ND}(F_h - F_l)$ і частота зламу F_C задані.

Середньоквадратичне (RMS) значення шуму в смузі частот визначається площею під кривою спектральної щільності шуму між верхньою F_h і нижньою F_l частотами смуги і записується у вигляді

$$\overline{U}(F_h, F_l, F_C)_{RMS} = \sqrt{\int_{F_l}^{F_h} \left(S_{ND}(F_h - F_l)\sqrt{\frac{F_C}{F}+1} \right)^2 dF} \text{ [В]}, \quad (8)$$

де $S_{ND}(F_h - F_l)$ – спектральна щільність білого шуму $\left[мкВ/\sqrt{Гц}\right]$; F_C – частота зламу [Гц]; F_l – нижня межа смуги частот [Гц]; F_h – верхня межа смуги частот [Гц].

Для оцінки калібрувальної характеристики СЩПШ квантового ГШ пропонується використовувати спрощений вираз (8), що приведений до смуги аналізу 1 Гц, в вигляді

$$S_U(F_h, F_l, F_C) = S_{ND}(F_h - F_l)^2 \left[F_C \ln\left(\frac{F_h}{F_l}\right) + F_h - F_l \right], \text{ [Вт/Гц]}. \quad (9)$$

Індивідуальні калібрувальні характеристики СЩПШ квантових ГШ пропонується отримувати методом звірення за допомогою компаратора шляхом застосування низькотемпературних мір (ГШ) державного первинного еталона спектральної щільності потужності шумового радіовипромінювання. Отримані оцінки СЩПШ $\vec{S} = [s_l]$ записують у таблицю калібрувальних параметрів квантового ГШ. Використовуючи вираз (9), апроксимують калібрувальні характеристики методом найменших квадратів в заданій смузі частот для оцінки невідомих характеристик спектральної щільності шуму $S_{ND}(F_h - F_l)$ і частоти зламу F_C .

Пропонується значення $S_{ND}(F_h - F_l)$ і F_C записувати або в таблицю електричних параметрів технічного опису криптографічного модуля, або представляти у вигляді графіка СЩПШ, що наводиться в розділі типових умов експлуатації. Так, використовуючи виконаний у логарифмічному масштабі графік СЩПШ (рис. 6 графік 4), можна знайти F_C на перетині ліній $S_{ND}(F_h - F_l)$ і $1/F$. При цьому квантові ГШ можна калібрувати спільно з вимірювачами коефіцієнта шуму серії NFA компанії Agilent або Keysight. Крім того, для отримання СЩПШ квантові ГШ повинні мати коаксіальний вихід для підключення до аналізаторів спектра серії ESA або аналізаторів сигналів MXA і EXA компанії Agilent або Keysight. Квантові джерела шуму повинні мати також можливість автоматичного вимірювання своєї власної шумової температури.

Висновки

Побудова прототипу КГВЧ нового покоління вимагає вирішення низки принципових фізичних і технічних задач. Важливим напрямком досліджень і створення ефективних квантових ГВП є розробка методів і засобів оцінки статистичних властивостей випадкових послідовностей. Статистичні показники мають вагомий вплив на загальну оцінку ефективності квантових ГВЧ. По суті, статистичні показники та побудовані на їх основі критерії оцінки є інструментом перевірки правильності технічних рішень щодо побудови квантових ГВП та забезпечення якості їх нерозрізнюваності. У більшості випадків дослідження статистичних властивостей здійснюється в рамках методики статистичних випробувань на основі статис-

тичних тестів. При цьому розробка методики, вибір статистичних тестів, створення інструментарію випробувань потребує перш за все аналізу самої природи випадковості.

Експериментальне підтвердження отриманих результатів було проведено на експериментальному зразку КД на парах рубідію. Аналіз отриманих результатів показав, що доступні через онлайн сервіси квантові генератори за результатами тестування згідно NIST (SP) 800-90A мають не гіршу нерозрізнюваність (випадковість) ніж запропонований КГВЧ.

Список літератури: 1. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І.Д. Горбенко. – Харків : Форт, 2012. – 878 с. 2. *Горбенко, Ю.І.* Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації : монографія. – Ч. 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем ; за заг. ред. І.Д. Горбенко. – Харків : Форт, 2016. – 960 с. 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. *Achleitner U.* Diploma Thesis, Innsbruck University (1997). 5. *Martino, A. J. , Morris, G. M*. Applied Optics 30, 981 (1991). 6. *Morris, G. M.* 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 до матеріалів: 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 до матеріалів: 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. – Vol. 20. – No. 11. –2012. 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 до матеріалів [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. *NIST* Special Publication (SP) 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [June 2012]. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf. 21. *Иванов, М. А., Чугунков, И. В*. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с. 22. *Тетерич, Н.М.* Генераторы шума и измерение шумовых характеристик. – М. : Энергия, 1968. – 216 с. 23. *Стандарты* частоты: принципы и приложения / Ф. Риле ; пер. с англ. Н. Н. Колачевского. – М. : Физматлит, 2009. – 511 с. 24. *Квантовая* радиофизика. Квантовые стандарты частоты с оптической накачкой : учеб. пособие / В.В. Семенов, Г.М. Смирнова, В.М. Хуторщиков ; С.-Петерб. гос. техн. ун-т СПб. : Изд-во СПбГТУ, 1999. – 536 с. 25. *Нарежний, А. П.* Идентификация скрытых периодичностей в нестационарных фазовых флуктуациях прецизионных мер частоты / А. П. Нарежний // Прикладная радиоэлектроника. – 2005. – Т.4. – № 2. – С. 148–152. 26. *Марал С.Л.* Цифровой спектральный анализ и его приложения. – М. : Мир, 1990. – 584 с. 27. *Stasev Yu.V., Kuznetsov A.A., Nosik A.M.* Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11.

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

Надійшла до редколегії 08.09.2016