

УДК 621.391

© А. А. Гавришев, 2024

ОЦЕНКА СВОЙСТВ ПОСЛЕДОВАТЕЛЬНОСТИ СЛУЧАЙНЫХ ЧИСЕЛ, ПОЛУЧЕННЫХ НА ОСНОВЕ КВАНТОВЫХ ПРОЦЕССОВ, С ПОМОЩЬЮ МЕТОДОВ НЕЛИНЕЙНОЙ ДИНАМИКИ

Из литературы известно, что многие из существующих алгоритмов генерации случайных чисел или псевдослучайных последовательностей не способны в полной мере обеспечить требуемый уровень безопасности, что послужило ключевой причиной развития генераторов случайных чисел или псевдослучайных последовательностей на новых принципах. Проведены исследования временных реализаций последовательности случайных чисел, полученных на основе квантовых процессов. Показано, что методы нелинейной динамики используются достаточно редко для исследования их свойств. Выполнено моделирование последовательности случайных чисел, полученных на основе квантовых процессов, и проведен количественно-качественный анализ их свойств с помощью методов нелинейной динамики. Установлено, что временные реализации последовательности случайных чисел, полученные на основе квантовых процессов, обладают повышенной скрытностью от постороннего наблюдателя и являются достаточно близкими к белому шуму. Указано, что такие последовательности случайных чисел, при соответствующей адаптации, могут найти применение для использования в современных системах передачи данных, т.к. обладают приемлемым значением пик-фактора.

Кл. сл.: случайные числа, квантовые процессы, нелинейная динамика, количественно-качественный анализ, свойства

ВВЕДЕНИЕ

Стремительная цифровизация общества и экономики играет первостепенную роль в увеличении спроса на повышение безопасности передаваемой информации, что служит дополнительным стимулом развития криптографии и скрытных систем связи. Известно [1–4], что для преобразования передаваемых данных к виду, который недоступен неавторизованному пользователю, используются в качестве исходных данных некоторые первичные состояния, создаваемые генераторами случайных чисел (СЧ) и псевдослучайных последовательностей (ПСЧ). Исходя из этого, защищенность передачи данных определяется в первую очередь качеством генерируемых СЧ и ПСЧ. Многие из существующих алгоритмов генерации СЧ или ПСЧ не способны в полной мере обеспечить требуемый уровень безопасности, что послужило ключевой причиной развития генераторов СЧ и ПСЧ на новых принципах [1–9], например на основе хаотических сигналов, на основе квантовых генераторов и др.

В последние годы один из наибольших интересов у специалистов вызывают исследования в области создания генераторов СЧ и ПСЧ, в основе работы которых лежат квантовые процессы [2, 5–

9]. Высокий уровень внутренней неопределенности этих процессов позволяет поддерживать генерацию некоррелированных случайных битов большой длины. Известны многочисленные конструкции таких генераторов, описанные в различных источниках [2, 5–9] и списках литературы к ним: основанные на регистрации времени детектирования одиночных фотонов, распределении числа одиночных фотонов, регистрации фазовых шумов и многие другие.

Одним из важных вопросов в данных условиях является вопрос, связанный с методами исследования свойств СЧ и ПСЧ, полученных на основе квантовых процессов. Анализ литературы показывает [2, 5–9], что для исследования свойств СЧ и ПСЧ, полученных на основе квантовых процессов, обычно используются следующие методы: временные и спектральные диаграммы, автокорреляционная функция, исследование закона распределения, количество и длина кодовых структур, статистические тесты NIST, DieHard и некоторые другие. Как видно, исследователи в основном используют стандартный набор известных методов. В данной работе авторы хотят расширить набор таких методов и провести оценку свойств СЧ и ПСЧ, полученных на основе квантовых процессов, с помощью методов нелинейной динамики.

ки. Указанные методы достаточно хорошо себя зарекомендовали в предыдущих работах авторов, например [3, 4, 11–14], однако не нашли широкого применения в указанной области.

Целью данной статьи является моделирование последовательности СЧ, полученных на основе квантовых процессов, и их количественно-качественный анализ с помощью методов нелинейной динамики.

ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

Проведем моделирование последовательности СЧ, полученных на основе квантовых процессов. Для генерирования таких чисел в качестве примера обратимся к работе [10]. В указанной работе описан квантовый генератор СЧ, основанный на квантовой случайности времени прихода фото-

нов. Основными характеристиками данного генератора СЧ являются высокая скорость генерации последовательностей и высокая степень их случайности, позволяющая в перспективе использовать его в системах криптографической защиты информации.

С помощью специального программного обеспечения, расположенного на ресурсе [15], авторами были сгенерированы 100 различных последовательностей СЧ, описанных в работе [10]. Пример полученной временной реализации приведен на рис. 1. Другие временные реализации имеют схожий вид.

На рис. 2 приведен пример спектральной диаграммы последовательности СЧ, полученных на основе квантовых процессов из работы [10], соответствующий рис. 1. Другие полученные спектральные диаграммы имеют схожий вид.

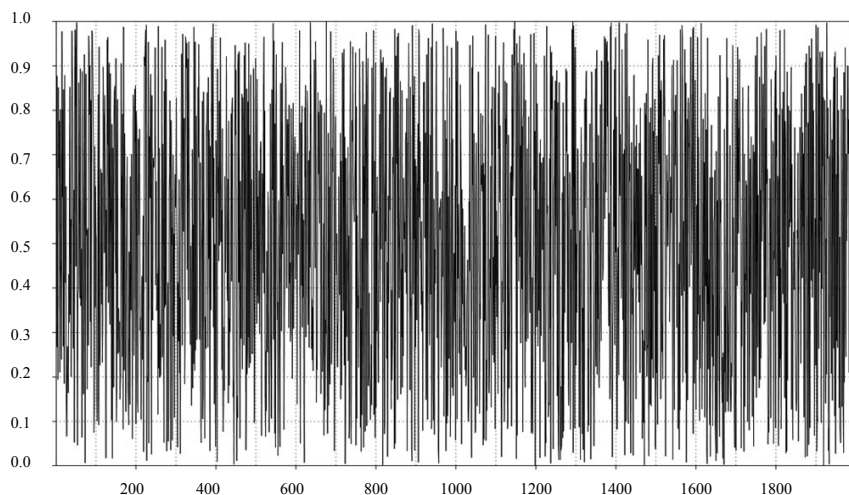


Рис. 1. Временная реализация последовательности СЧ, полученных на основе квантовых процессов из работы [10]

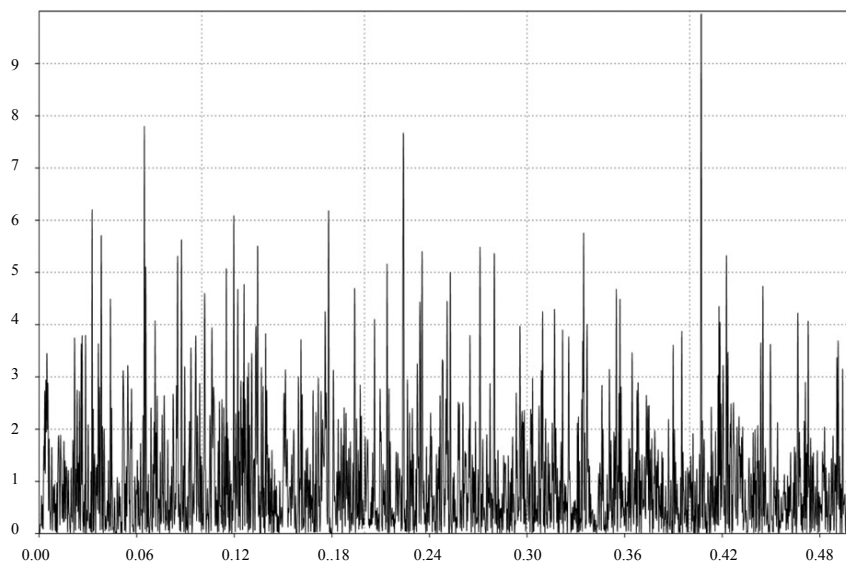


Рис. 2. Спектральная диаграмма последовательности СЧ, полученных на основе квантовых процессов из работы [10]

Табл. 1. Некоторые из методов нелинейной динамики, применяемые для оценки свойств СЧ, полученных на основе квантовых процессов из работы [10]

№	Название метода	Обозначение	Формульное выражение
1	BDS-статистика	$\overline{w(\varepsilon)}$	$w_{m,N}(\varepsilon) = \sqrt{N-m+1} \frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}$
2	Показатель Херста	H	$R / S = (\tau / 2)^H$
3	Пик-фактор	P	$P = \frac{U_{\max}}{\sigma}$

Табл. 2. Рассчитанные значения BDS-статистики $\overline{w(\varepsilon)}$, показателя Херста H и пик-фактора P временных реализаций СЧ, полученных на основе квантовых процессов из работы [10]

Название	Значение BDS-статистики $\overline{w(\varepsilon)}$	Значение показателя Херста H	Значение пик-фактора P
СЧ, полученные на основе исследуемых квантовых процессов	[0.15, 1.95]	[0.46, 0.60]	[3.3, 3.5]

Как видно из рис. 1, 2, последовательности СЧ, полученные на основе квантовых процессов из работы [10], имеют сложный шумоподобный вид. Таким образом, на качественном уровне они являются близкими к белому шуму. Полученные результаты в целом совпадают с известными исследованиями [2, 5–9].

Далее проведем количественную оценку последовательностей СЧ, полученных на основе квантовых процессов из работы [10], с помощью некоторых из известных методов нелинейной динамики, приведенных в табл. 1. Более подробно с ними возможно ознакомиться в работах [1, 3, 4, 11–14].

BDS-статистика основана на статистической величине $\overline{w(\varepsilon)}$:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1} \frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \quad (1)$$

где $C_{m,N}(\varepsilon)$ и $C_{1,N-m}(\varepsilon)$ — корреляционные интегралы, а $\sigma_{m,N}(\varepsilon)$ — среднеквадратическое отклонение.

Показатель Херста H описывается выражением, представленным формулой (2):

$$R / S = (\tau / 2)^H, \quad (2)$$

где R — нормированный размах вариации (разность максимального и минимального значений измеряемого параметра), S — стандартное отклонение (корень квадратный от дисперсии), τ — период (длина ряда) наблюдений.

Пик-фактор сигнала вычисляется с помощью следующего выражения (3):

$$P = \frac{U_{\max}}{\sigma}, \quad (3)$$

где $U_{\max}$ — максимальное значение сигнала, σ — среднеквадратичное значение сигнала.

В табл. 2 приведены рассчитанные значения BDS-статистики, показателя Херста и пик-фактора для временных реализаций последовательности СЧ, полученных на основе квантовых процессов из работы [10].

Как видно из табл. 2, временные реализации последовательностей СЧ, полученных на основе квантовых процессов из работы [10], обладают значениями BDS-статистики $\overline{w(\varepsilon)} \in [0.15, 1.95]$. Согласно известным исследованиям [3, 4, 11–13], это указывает на то, что временные реализации последовательности СЧ, полученных на основе квантовых процессов из работы [10], обладают повышенной скрытностью от постороннего наблюдателя, т.к. их значение BDS-статистики $\overline{w(\varepsilon)} \leq 1.96$. Указанный интервал определяет сигналы, подобные белому шуму. Также из табл. 2 видно, что временные реализации последовательности СЧ, полученных на основе квантовых процессов из работы [10], обладают значениями показателя Херста $H \in [0.46, 0.60]$, что так же указывает [3, 4, 11–13] на то, что такие СЧ подобны белому шуму, т.к. находятся около значений показателя

Херста $H \approx 0.5$. Таким образом, показатель Херста также указывает на то, что такие последовательности СЧ обладают повышенной скрытностью от постороннего наблюдателя. Кроме этого, данные из табл. 2 показывают, что временные реализации последовательности СЧ, полученных на основе квантовых процессов из работы [10], обладают значением пик-фактора $P \in [3.3, 3.5]$. Полученные значения показывают, что такие последовательности СЧ при соответствующей адаптации могут найти применение для использования в современных системах передачи данных, т.к. обладают приемлемым значением пик-фактора ($P < 4$). Полученные результаты в целом совпадают с известными исследованиями [2, 5–9].

ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе проведены исследования временных реализаций последовательности СЧ, полученных на основе квантовых процессов. Показано, что методы нелинейной динамики используются достаточно редко для исследования свойств таких СЧ. Выполнено моделирование последовательности СЧ, полученных на основе квантовых процессов из работы [10], и проведен количественно-качественный анализ ее свойств с помощью временных и спектральных диаграмм, BDS-статистики, показателя Херста и пик-фактора. В результате проведенных исследований установлено, что временные реализации последовательности СЧ, полученных на основе квантовых процессов из работы [10], обладают повышенной скрытностью от постороннего наблюдателя и являются достаточно близкими к белому шуму. Кроме этого, показано, что такие последовательности СЧ при соответствующей адаптации могут найти применение для использования в современных системах передачи данных. Полученные результаты в целом совпадают с известными исследованиями [2, 5–9].

Основываясь на полученных результатах, автор считает перспективным использовать такие последовательности СЧ не только для систем криптографической защиты информации, но и для современных систем передачи данных. Кроме того, перспективным видится более широкое внедрение методов нелинейной динамики для исследования свойств различных типов СЧ и ПСЧ.

СПИСОК ЛИТЕРАТУРЫ

1. Сухарев Е.М., ред. Общесистемные вопросы защиты информации. Коллективная монография. Кн. 1. М.: Радиотехника, 2003. 292 с.

2. Петренко А.А., Ковалев А.В., Бугров В.Е. Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 962–968. DOI: 10.17586/2226-1494-2021-21-6-962-968
3. Гавришнев А.А., Осипов Д.Л. Построение обобщенного критерия оценки качества криптостойких кодовых последовательностей, используемых в защищенных беспроводных системах связи // Научное приборостроение. 2023. Т. 33, № 4. С. 111–118. URL: <http://iairas.ru/mag/2023/abst4.php#abst11>
4. Гавришнев А.А. Моделирование и количественно-качественный анализ распространенных защищенных систем связи // Прикладная информатика. 2018. Т. 13, № 5 (77). С. 84–122. URL: http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=2300
5. Орлов М.А., Нечаев К.А., Резниченко С.А. Оценка статистических свойств и криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM // Безопасность информационных технологий. 2023. № 1. С. 14–26. DOI: 10.26583/bit.2023.1.01
6. Балыгин К.А., Зайцев В.И., Климов А.Н., Кулик С.П., Молотков С.Н. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с // ЖЭТФ. 2018. Т. 153, № 6. С. 879–894. DOI: 10.7868/S0044451018060044
7. Архангельская А.В. Построение высокоскоростных квантовых генераторов случайных чисел для систем защиты информации. Автореф. дис. ...канд. техн. наук. 2008. 17 с.
8. Kravtsov K.S., Kulik S.P., Radchenko I.V. Quantum random number generator // Матем. вopr. криптогр. 2016. Т. 7, № 2. С. 111–114. DOI: 10.4213/mvk188
9. Aguirre S., Arango-Montoya J.D., Jaramillo-Duque D., Méndez J.F., Morales-Durán N., Restrepo M. A quantum random number generator implementation with polarized photons // Emergent Scientist. 2017. Vol. 1, no. 2. 8 p. DOI: 10.1051/emsci/2017002
10. Miszczak J.A. Employing online quantum random number generators for generating truly random quantum states in Mathematica // Computer Physics Communications. 2013. Vol. 184, iss. 1. P. 257–258. DOI: 10.1016/j.cpc.2012.08.012
11. Гавришнев А.А. К вопросу об использовании гиперхаотических сигналов для передачи данных в системах радиосвязи // Научное приборостроение. 2023. Т. 33, № 2. С. 62–74. URL: <http://iairas.ru/mag/2023/abst2.php#abst6>
12. Гавришнев А.А., Осипов Д.Л. Оценка скрытности OFDM-сигналов, основанных на BPSK модуляции, с помощью методов нелинейной динамики // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 9. С. 13–19. URL: <https://cyberleninka.ru/article/n/otsenka-skrytnosti-ofdm-signalov-osnovannyh-na-bpsk-modulyatsii-s-pomoschyu-metodov-nelineynoy-dinamiki>

13. Гавришев А.А., Гавришев А.Н. К вопросу о расчете значений пик-фактора сигналов, генерируемых распространёнными скрытными системами связи // Вестник НЦБЖД. 2020. № 3 (45). С. 149–157. URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2478119.pdf
14. Гавришев А.А., Осипов Д.П. Анализ свойств сверхширокополосных сигналов, влияющих на скрытность и надёжность передачи данных в системах радиосвязи // Научное приборостроение. 2024. Т. 34, № 2. С. 112–120. URL: <http://iairas.ru/mag/2024/abst2.php#abst11>
15. QRNGHuBerlinTest. URL: <https://github.com/SeppPenner/QRNGHuBerlinTest?ysclid=m1himeb6rq277959768>

Московский государственный лингвистический университет, Москва

Контакты: Гавришев Алексей Андреевич,
alexxx.2008@inbox.ru

Материал поступил в редакцию 17.09.2024

EVALUATION OF THE PROPERTIES OF A SEQUENCE OF RANDOM NUMBERS OBTAINED ON THE BASIS OF QUANTUM PROCESSES USING NONLINEAR DYNAMICS METHODS

A. A. Gavrishchev

MSLU, Moscow, Russia

It is known from the literature that many of the existing algorithms for generating random numbers or pseudorandom sequences are not able to fully provide the required level of security, which was the key reason for the development of random number generators or pseudorandom sequences based on new principles. Studies of time realizations of random numbers obtained on the basis of quantum processes have been carried out. It is shown that the methods of nonlinear dynamics are rarely used to study the properties of such random numbers. The simulation of a sequence of random numbers obtained on the basis of quantum processes is carried out, and a quantitative and qualitative analysis of their properties using methods of nonlinear dynamics is carried out. It has been revealed that the time realizations of random numbers obtained on the basis of quantum processes have increased stealth from an outside observer and are quite close to white noise. It is indicated that such random numbers, after appropriate adaptation, can find application for use in modern data transmission systems since they have an acceptable peak factor value.

Keywords: random numbers, quantum processes, nonlinear dynamics, quantitative and qualitative analysis, properties

REFERENCES

1. Sukharev E.M., editor. *Obshchesistemnye voprosy zashchity informatsii. Kollektivnaya monografiya. Kn. 1* [System-wide issues of information protection. Collective monograph. Book 1]. Moscow, Radiotekhnika Publ., 2003. 292 p. (In Russ.).
2. Petrenko A.A., Kovalev A.V., Bougrov V.E. [Random number generation with arrays of coupled quantum-dot micropillar lasers]. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2021, vol. 21, no 6, pp. 962–968. (In Russ.). DOI: 10.17586/2226-1494-2021-21-6-962-968
3. Gavrishchev A.A., Osipov D.L. [Building of a generalized quality assessment criterion cryptographic code sequences used in secure wireless communication systems]. *Nauchnoe Priborostroenie* [Scientific Instrumentation], 2023, vol. 33, no. 4, pp. 111–118. (In Russ.). URL: <http://iairas.ru/mag/2023/abst4.php#abst11>
4. Gavrishchev A.A. [Modeling and quantitative and qualitative analysis of common secure communication systems]. *Prikladnaya informatika* [Journal of applied informatics], 2018, vol. 13, no. 5 (77), pp. 84–122. (In Russ.). URL: http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=2300
5. Orlov M.A., Nechaev K.A., Reznichenko S.A. [Evaluation of statistical properties and cryptographic strength of random sequences obtained by an IBM quantum computer]. *Bezopasnost' informatsionnykh tekhnologii* [IT Security (Russia)], 2023, no. 1, pp. 14–26. (In Russ.). DOI: 10.26583/bit.2023.1.01
6. Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N. [A quantum random number generator based on the 100-mbit/s poisson photocount statistics]. *Zhurnal eksperimental'noj i teoreticheskoy fizik* [Journal of Experimental and Theoretical Physics], 2018, vol. 153, no. 6, pp. 879–894. (In Russ.). DOI: 10.7868/S0044451018060044
7. Arkhangel'skaya A.V. *Postroenie vysokoskorostnykh kvantovykh generatorov sluchainykh chisel dlya sistem zashchity informatsii*. Avtoref. diss. kand. techn. nauk [Construction of high-speed quantum random number generators for information protection systems. Autoref. cand. techn. sci. diss.]. 2008. 17 p. (In Russ.).
8. Kravtsov K.S., Kulik S.P., Radchenko I.V. [Quantum random number generator]. *Matematicheskie voprosy kriptografii* [Mathematical aspects of cryptography], 2016, vol. 7, no. 2, pp. 111–114. (In Russ.). DOI: 10.4213/mvk188
9. Aguirre S., Arango-Montoya J.D., Jaramillo-Duque D., Méndez J.F., Morales-Durán N., Restrepo M. A quantum random number generator implementation with polarized photons. *Emergent Scientist*, 2017, vol. 1, no. 2, 8 p. DOI: 10.1051/emsci/2017002
10. Miszczak J.A. Employing online quantum random number generators for generating truly random quantum states in Mathematica. *Computer Physics Communications*, 2013, vol. 184, no. 1, pp. 257–258. DOI: 10.1016/j.cpc.2012.08.012
11. Gavrishchev A.A. [On the use of hyperchaotic signals for data transmission in radio communication systems]. *Nauchnoe Priborostroenie* [Scientific Instrumentation], 2023, vol. 33, no. 2, pp. 62–74. (In Russ.). URL: <http://iairas.ru/mag/2023/abst2.php#abst6>

12. Gavrishev A.A., Osipov D.L. [Evaluation of the stealth of OFDM-signals based on BPSK modulation, using non-linear dynamics methods]. *T-Comm: Telekommunikatsii i transport* [T-Comm], 2022, vol. 16, no. 9, pp. 13–19. URL: <https://cyberleninka.ru/article/n/otsenka-skrytnosti-ofdm-signalov-osnovannyh-na-bpsk-modulyatsii-s-pomoschu-metodov-nelineynoy-dinamiki> (In Russ.).
13. Gavrishev A.A., Gavrishev A.N. [To the question of calculating the crest factor values of signals generated by common hidden communication systems]. *Vestnik NTSBZHD* [NCBWC Bulletin], 2020, no. 3 (45), pp. 149–157. (In Russ.). URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2478119.pdf
14. Gavrishev A.A., Osipov D.L. [Analysis of the properties of ultra-wideband signals affecting the secrecy and reliability of data transmission in radio communication systems]. *Nauchnoe Priborostroyeniye* [Scientific Instrumentation], 2024, vol. 34, no. 2, pp. 112–120. (In Russ.). URL: <http://iairas.ru/mag/2024/abst2.php#abst11>
15. *QRNGHuBerlinTest*. URL: <https://github.com/SeppPenner/QRNGHuBerlinTest?ysclid=m1himeb6rq277959768>

Contacts: *Gavrishev Aleksey Andreevich*,
alexxx.2008@inbox.ru

Article received by the editorial office on 17.09.2024

INTRODUCTION

The rapid digitalization of society and the economy plays a primary role in increasing the demand for advanced security of information transmission, which serves as an additional incentive for the development of cryptography and covert communication systems. It is known [1–4] that to convert transmitted data into a form that is inaccessible to an unauthorized user, some primary states created by random number generators (RNG) and pseudo-random sequences (PRS) are used as initial data. Based on this, the security of data transmission is determined primarily by the quality of the generated RN and PRS. A lot of the existing algorithms for generating RN or PRS are not able to fully ensure the required level of safety, which is the key reason for the development of RN and PRS generators using new principles [1–9], e.g., based on chaotic signals, based on quantum generators, etc.

In recent years, one of the greatest interests among specialists has been research in the field of creating RN and PRS generators, the work of which is based on quantum processes [2, 5–9]. The high level of internal uncertainty of these processes allows the generation of uncorrelated random bits of large length to be supported. Numerous designs of such generators are known, described in various sources [2, 5–9] and reference lists to them: based on the record of the detection time of single photons, the distribution of the number of single photons, the record of phase noise, and many others.

One of the important questions in these conditions is the question related to the methods of studying the properties of RN and PRS obtained on the basis of quantum processes. Literature analysis shows [2, 5–9] that for the study of RN and PRS properties derived from quantum processes, the following methods are usually used: time and spectral diagrams, autocorrelation function, study of the distribution law, number and length of code structures, NIST statistical tests, DieHard, and several others. As you can see, researchers mainly use a standard set of known methods. In this work, the authors want to expand the set of such methods and assess the properties of RN and PRS obtained on the basis of quantum processes using methods of nonlinear dynamics. These methods have proven themselves quite well in the previous works of the authors, for example, [3, 4, 11–14] but have not been widely used in this field.

The purpose of this article is to model the RN sequence obtained on the basis of quantum processes and their quantitative and qualitative analysis using nonlinear dynamics methods.

RESEARCH PART

We simulate the RN sequence obtained on the basis of quantum processes. To generate such numbers,

as an example, let us turn to [10]. This work describes a quantum RN generator, based on quantum randomness of time of arrival photons. The main characteristics of this RN generator are the high speed of generating sequences and a high degree of their randomness, which opens perspective for using it in cryptographic information protection systems.

Using special software located on the resource [15], the authors generated 100 different RN sequences described in [10]. An example of the resulting time implementation is shown in Fig. 1. Other time implementations are similar.

Fig. 1. Time implementation of the sequence of RN obtained on the basis of quantum processes, as shown in [10]

Fig. 2 shows an example of a spectral diagram of the RN sequence obtained based on quantum processes from [10], corresponding to Fig. 1. Other obtained spectral diagrams have a similar appearance.

Fig. 2. Spectral diagram of the sequence of RN obtained on the basis of quantum processes from the work [10]

As can be seen from Figs. 1, 2, the RN sequences obtained on the basis of quantum processes from work [10], have a complex noise-like appearance. Thus, on a qualitative level, they are close to white noise. The results obtained generally coincide with the known studies [2, 5–9].

Next, we quantify the RN sequences obtained on the basis of quantum processes from the work [10] using some of the well-known methods of nonlinear dynamics given in Tab. 1. You can learn more about them in [1, 3, 4, 11–14].

Tab. 1. Some of the methods of nonlinear dynamics used to assess the properties of RN obtained based on quantum processes from work [10]

BDS statistics are based on the statistical value:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1} \frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \quad (1)$$

where $C_{m,N}(\varepsilon)$ and $C_{1,N-m}(\varepsilon)$ are the correlation integrals and $\sigma_{m,N}(\varepsilon)$ is the standard deviation.

The Hurst exponent H is described by the expression represented by formula (2):

$$R / S = (\tau / 2)^H, \quad (2)$$

where R is the normalized range of variation (the difference between the maximum and minimum values of the measured parameter), S — the standard deviation (square root of the variance), τ — the period (row length) of observations.

The peak factor of the signal is calculated using the following expression (3):

$$P = \frac{U_{\max}}{\sigma}, \quad (3)$$

where $U_{\max}$ is the maximum value of the signal, σ is the mean square value of the signal.

Tab. 2 shows the calculated values of BDS statistics, Hurst index, and peak factor for time implementations of the RN sequence obtained on the basis of quantum processes from the work [10].

Tab. 2. Calculated values of BDS statistics $\overline{w(\varepsilon)}$, Hurst H index, and peak factor P of time realizations of RN obtained on the basis of quantum processes from the work [10]

As can be seen from Tab. 2, the time realizations of the RN sequences obtained on the basis of quantum processes from the work [10] have the values of BDS statistics $\overline{w(\varepsilon)} \in [0.15, 1.95]$. According to known studies [3, 4, 11–13], this indicates that the time realizations of the RN sequences obtained on the basis of quantum processes from the work [10] have an increased secrecy from an outside observer, since their BDS statistics value is $\overline{w(\varepsilon)} \leq 1.96$. This interval defines signals similar to white noise. It can also be seen from Tab. 2 that the time realizations of the RN sequence obtained on the basis of quantum processes from the work [10] have the values of the Hurst index

$H \in [0.46, 0.60]$, which also indicates [3, 4, 11–13] that such RNs are similar to white noise, since they are close to the Hurst index value $H \approx 0.5$. Thus, the Hurst index also indicates that such sequences of RN have an increased stealth from an outside observer. In addition, the data from Tab. 2 show that the time realizations of the RN sequence obtained based on quantum processes from [10], have a peak factor value $P \in [3.3, 3.5]$. The obtained values reveal that such RN sequences, with appropriate adaptation, can be used in modern data transmission systems since they have an acceptable peak factor value ($P < 4$). The results obtained generally coincide with the known studies [2, 5–9].

CONCLUSION

Thus, in this work, studies of time implementations of the RN sequence obtained on the basis of quantum processes were carried out. It has been shown that nonlinear dynamics methods are rarely used to study the properties of such RN. The sequence of RN obtained based on quantum processes from work [10], and a quantitative and qualitative analysis of its properties was carried out using time and spectral diagrams, BDS statistics, the Hurst index and the peak factor. As a result of the studies, it was found that the time implementations of the RN sequence obtained on the basis of quantum processes from the work [10] have an increased secrecy from extraneous observers and are reasonably close to white noise. In addition, it is shown that such RN sequences with appropriate adaptation can be used in modern data transmission systems. The results obtained generally coincide with the known studies [2, 5–9].

Based on the results obtained, the author considers it promising to use such RN sequences not only for cryptographic information protection systems but also for modern data transmission systems. In addition, the wider introduction of nonlinear dynamics methods for studying the properties of various types of RN and PRS seems promising.