http://dx.doi.org/10.35596/1729-7648-2023-21-3-34-40

Оригинальная статья
Original paper

УДК 621.382.2/.3

СТАБИЛЬНОСТЬ ХАРАКТЕРИСТИК ФИЗИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

М. О. ПИКУЗА[1], С. Ю. МИХНЕВИЧ[2], А. Ю. СЕНКЕВИЧ[2]

[1]«КБ Радар» – управляющая компания холдинга «Системы радиолокации» (г. Минск, Республика Беларусь)
[2]Белорусская государственная академия связи (г. Минск, Республика Беларусь)

Поступила в редакцию 13.02.2023

Аннотация. Развитие технологий приводит к необходимости пересмотра используемых методов получения криптографических ключей. На параметры случайности последовательностей, сгенерированных физическими генераторами случайных последовательностей, влияют физические параметры регистрирующей аппаратуры и окружающей среды. Получены требования к случайности последовательности при прохождении бинарного теста. Продемонстрировано, что с увеличением длины последовательности требования к возможным отклонениям от равновероятного распределения 0 и 1 возрастают. Оценена стабильность случайности последовательностей, выданных генератором на основе изучения фотонов. Исследуемый генератор состоит из светодиода и кремниевого малогабаритного фотоумножителя, предназначенного для регистрации светового излучения малой мощности. Показаны возможные физические процессы, приводящие к ухудшению случайности последовательностей. Оценена возможность использования генератора случайных числовых последовательностей на основе кремниевого малогабаритного фотоумножителя для криптографических целей.

Ключевые слова: случайная бинарная последовательность, генератор случайных чисел, кремниевый фотоумножитель, достоверность теста, бинарный тест, криптографический ключ.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Пикуза, М. О. Стабильность характеристик физических генераторов случайных чисел / М. О. Пикуза, С. Ю. Михневич, А. Ю. Сенкевич // Доклады БГУИР. 2023. Т. 21, № 3. С. 34–40. http://dx.doi.org/10.35596/1729-7648-2023-21-3-34-40.

STABILITY OF CHARACTERISTICS OF PHYSICAL RANDOM NUMBER GENERATORS

MAKSIM O. PIKUZA[1], SVETLANA YU. MIKHNEVICH[2], ALIONA YU. SIANKEVICH[2]

[1]"KB Radar" – Managing Director Holding Company of "Radar Systems" (Minsk, Republic of Belarus)
[2]Belarusian State Academy of Communications (Minsk, Republic of Belarus)

Submitted 13.02.2023

Abstract. The development of technologies leads to the need of revising the methods used to obtain cryptographic keys. The randomness parameters of sequences generated by physical random sequence generators are affected by the physical parameters of the recording equipment and the environment. The requirements for the randomness of the sequence, when passing the binary test, are obtained. It is shown that as the sequence length increases, the requirements for possible deviations from the equiprobable distribution of 0 and 1 increase. The randomness stability of the sequences generated by the generator based on the study of photons is estimated. The oscillator under study

consists of an LED and a compact silicon photomultiplier designed to detect low-power light radiation. Possible physical processes leading to the deterioration of the randomness of sequences are shown. The possibility of using a generator of random numerical sequences based on a small-sized silicon photomultiplier for cryptographic purposes is estimated.

Keywords: random binary sequence, random number generator, silicon photomultiplier, test reliability, binary test, cryptographic key.

Conflict of interests. The authors declare no conflict of interests.

For citation. Pikuza M. O., Mikhnevich S. Yu., Siankevich A. Yu. (2023) Stability of Characteristics of Physical Random Number Generators. *Doklady BGUIR*. 21 (3), 34–40. http://dx.doi.org/10.35596/1729-7648-2023-21-3-34-40 (in Russian).

Введение

Развитие квантовых технологий приводит к появлению новых направлений техники и технологий, вместе с тем в некоторых направлениях будет происходить замена или вытеснение существующих технологий. Так, в области криптографии уже сейчас встает вопрос о возможности применения квантовых компьютеров для раскрытия криптографических ключей и, следовательно, для расшифровки сообщений. Таким образом, некоторые криптографические алгоритмы становятся ненадежными при использовании квантовых компьютеров [1]. Учитывая, что начинается создание и поставка на рынок серийных квантовых компьютеров, вопрос надежности криптографических ключей и алгоритмов становится актуальным.

В [1–3] показано, что непредсказуемость случайных процессов может быть обусловлена квантовыми процессами или математической сложностью задачи, связанной с техническими (временными или ресурсными) ограничениями настоящего уровня развития технологий. Поскольку математическая сложность задачи – временная трудность – в большинстве случаев преодолевается развитием технологий (или появлением квантового компьютера), становятся актуальными поиск и разработка надежных физических источников случайных бинарных последовательностей на основе квантовых процессов.

Физические источники случайных последовательностей в основном зависят от параметров окружающей среды, а на сами последовательности влияет регистрирующая и обрабатывающая аппаратура [3]. Поэтому любое изменение может привести к нестабильности последовательности битов и, следовательно, к ухудшению случайности. Изменение параметров случайности в течение времени работы генератора приведет к его ненадежности. В литературе встречаются рекомендации тестировать физические генераторы случайных чисел до и в процессе работы [3].

Проведение исследований

Тестирование случайных последовательностей осуществляется методами на основе серии тестов, приведенных в NIST или FIPS [4, 5]. Согласно этим методикам, тестирование для криптографических целей должно проводиться на последовательности минимум 10^6 бит и с уровнем достоверности теста $\alpha = 0{,}01$. В любом тесте вычисляют вероятность получения неслучайной последовательности $(1 - P)$, т. е. отличие случайности идеального генератора (полученной методами математической статистики) и случайности проверяемой последовательности с учетом типа оцениваемой данным тестом неслучайности. Если $P > \alpha$, считается, что последовательность с точностью α случайна [4].

Бинарный, или статистический, тест на равновероятность появления 0 и 1 входит в обе серии тестов. Исследуем влияние нестабильности параметров генератора случайных чисел с помощью бинарного теста. Расчет значения P проводится следующим образом. В бинарном тесте в случайной последовательности «0» заменяется на «–1» и находится сумма ряда *Sum* размера ряда n. Далее вычисляется статистический параметр теста

$$S_n = \frac{Sum}{\sqrt{2n}} \tag{1}$$

и рассчитывается P через дополнительную функцию ошибок

$$P(S_n) = \frac{2}{\sqrt{\pi}} \int_{S_n}^{\infty} e^{-t^2} dt. \tag{2}$$

Если $P > 0{,}01$, то случайная последовательность генерируется с достоверностью 99 %, если $P > 0{,}001$ – с достоверностью 99,9 % [4]. На рис. 1 приведена функция ошибок от величин S_n, для которой значения $P(S_n) < 0{,}01$ проходят тест.

Рис. 1. Функция ошибок
Fig. 1. Error function

На рис. 2 приведен график зависимости максимального значения суммы ряда *Sum*, при которой последовательность проходит тест с определенным уровнем достоверности α, от размера ряда *n*. Максимальные значения суммы ряда *Sum* от размера ряда *n* приведены в табл. 1.

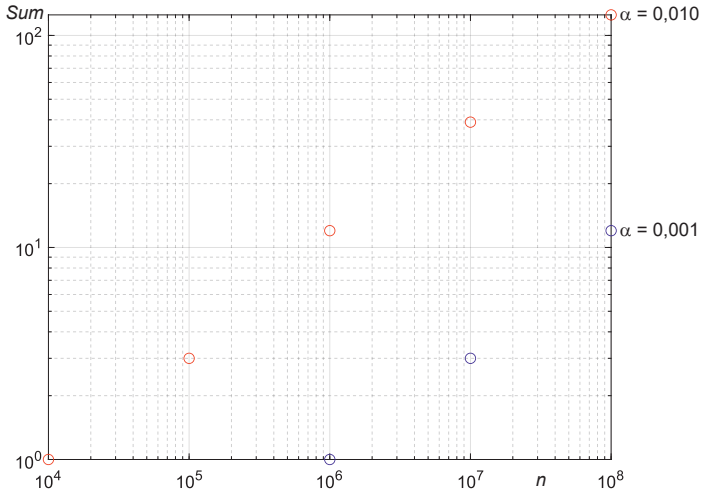

Рис. 2. Зависимость максимального значения суммы ряда *Sum* от размера ряда *n*
Fig. 2. Dependence of the maximum value of the sum of the series *Sum* on the size of the series *n*

Таблица 1. Максимальные значения суммы ряда *Sum* в зависимости от размера ряда *n*
Table 1. Maximum values of the sum of the series *Sum* depending on the size of the series *n*

α = 0,010	*n*	1,0000e + 04	1,0000e + 05	1,0000e + 06	1,0000e + 07	1,0000e + 08
	Sum	1,0000e + 00	3,0000e + 00	1,2000e + 01	3,9000e + 01	1,2500e + 02
α = 0,001	*n*	1,0000e + 04	1,0000e + 05	1,0000e + 06	1,0000e + 07	1,0000e + 08
	Sum	0	0	1,0000e + 00	3,0000e + 00	1,2000e + 01

Зависимость максимального значения суммы ряда в логарифмическом масштабе от длины числовой последовательности практически линейна, но коэффициент пропорциональности

не равен единице. Так, для прохождения теста последовательности длиной 10^5 максимальное количество отклонений суммы от нуля должно по модулю равняться 3, т. е. разница допустимой ошибки и длины последовательности составляет 4 порядка. Это значит, что с учетом четности числа знаков в последовательности допускается замена всего лишь одного значения бита противоположным. При последовательности длиной 10^8 максимальное количество отклонений суммы от нуля должно по модулю быть равно 125, т. е. разница – 5 порядков. С учетом четности числа знаков в последовательности допускается замена значений 62 битов противоположными. Таким образом, с увеличением длины последовательности требования к точности возрастают. При тестировании последовательностей для криптографических целей необходимая минимальная длина последовательности составляет 10^6 знаков.

Оценим требуемую стабильность параметров физических источников на примере генератора случайных чисел (рис. 3) на основе квантового явления – излучения единичных фотонов при фотоэффекте [6, 7]. Схема устройства, представленного на рис. 3, состоит из светодиода, испускающего излучение, и детектора излучения.

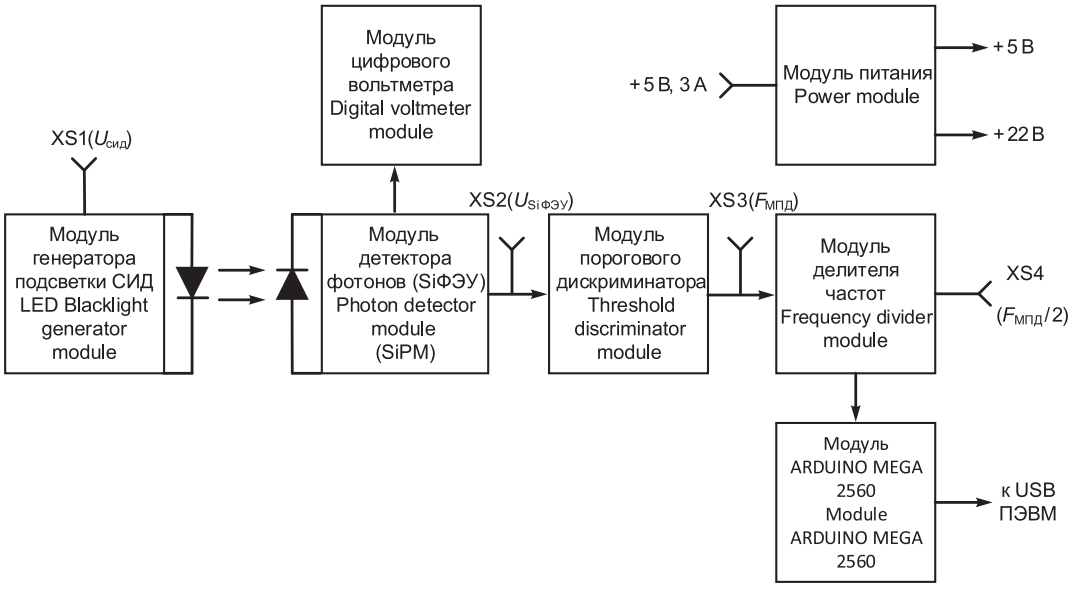

Рис. 3. Схема генератора случайных чисел
Fig. 3. Random number generator circuit

Лавинные фотодиоды (ЛФД) используют в волоконно-оптических линиях связи в качестве детекторов фотонов в криптографических системах. В настоящее время выпускаются кремниевые и германиевые ЛФД. Изучению характеристик кремниевых ЛФД посвящен ряд работ, например [8–12]. Серию кремниевых малогабаритных фотоумножителей также выпускает ОАО «Интеграл».

Параметры кремниевых малогабаритных фотоумножителей (КОФ5-1035, КОФ5-1035А) отличаются от лавинных фотодиодов (КОФ104К1, КОФ104К2, КОФ101Г, КОФ101Г1, КОФ101, КОФ102В, КОФ102В1), выпускаемых ОАО «Интеграл». Лавинные фотодиоды в основном характеризуются малыми коэффициентами умножения (до 100), высокими рабочими напряжениями (180–300 В) и низкой чувствительностью к световому потоку (0,30–0,75 А/Вт). ЛФД предназначены для использования в устройствах оптической локации, дальномерах, для регистрации ионизирующих излучений, в качестве альтернативы фотоэлектронным умножителям. Кремниевый малогабаритный фотоумножитель является функциональным аналогом многопиксельного счетчика фотонов фирмы Hamamatsu (Multi-Pixel Photon Counter, MPPC), он также называется кремниевым фотоумножителем (Silicon Photomultiplier, SiPM).

В приведенной на рис. 3 схеме использовался кремниевый малогабаритный фотоумножитель из пробной партии, который по характеристикам отличался напряжением пробоя. В соответствии с техническими документами основой кремниевых фотоумножителей КОФ5-1035 и КОФ5-1035А является кристалл кремния, на который нанесены пиксели размером 35×35 мкм, являющиеся

лавинными фотодиодами. ЛФД работают в «режиме Гейгера», т. е. при обратном напряжении, превышающем напряжение пробоя, что позволяет получать коэффициент усиления 10^5–10^6. Единичный импульс генерируется детектируемыми фотонами и гасится подключенным к каждому лавинному фотодиоду резистором. Пиксели (лавинные фотодиоды) выполнены из Ti и AlCu на планарной стороне и из Ti, Ni, Ag – на непланарной. Все пиксели через сопротивление соединены в единый канал. Общий выходной сигнал кремниевого фотоумножителя представляет собой сумму выходных сигналов с каждого пикселя. Кремниевые фотоумножители обладают высокой обнаружительной способностью, необходимой для счета фотонов, и используются в различных применениях, в которых требуется детектирование очень слабых световых сигналов на уровне единичных фотонов. Кремниевые фотоумножители КОФ5-1035, КОФ5-1035А характеризуются следующими параметрами:

– диапазоном длин волн – от 380 мкм до 800 нм;
– диапазоном напряжения смещения (выше Ub) – 1–5 В;
– коэффициентом усиления – не менее 10^6;
– эффективностью регистрации фотонов (PDE) – не менее 30 %;
– диапазоном рабочих температур среды – от минус 10 до плюс 70 °С;
– повышенной предельной температурой среды 100 °С.

Кремниевые фотоумножители КОФ5-1035, КОФ5-1035А используют для регистрации излучения низкой интенсивности. Однако есть вопрос о возможности их применения в схемах генераторов случайных числовых последовательностей. Результаты проведенных экспериментов по тестированию случайных последовательностей, сгенерированных исследуемым генератором, показывают достаточно хорошую случайность (на длине последовательности $3 \cdot 10^3$ и при $\alpha = 0{,}1$). Вместе с тем при определении качества случайных последовательностей в соответствии с требованиями NIST для криптографических целей (на длине последовательности 10^6 и при $\alpha = 0{,}010$–$0{,}001$) последовательности проходят тест только в случае очень точной настройки перенапряжения, подаваемого на фотоумножитель, и тока, проходящего через светодиод.

В соответствии с технической документацией коэффициент усиления рассматриваемых фотоумножителей зависит от перенапряжения линейно. При изменении перенапряжения (напряжения более напряжения пробоя, определенного экспериментально как 21 В [9, 10]) от 1,2 до 2,8 В коэффициент усиления меняется приблизительно от $3 \cdot 10^5$ до 10^6, т. е. почти в 3 раза. Температурная зависимость коэффициента усиления имеет нелинейный характер [9] и в диапазоне температур 293–298 К изменяется примерно на 10 %.

В исследуемой схеме напряжение считывания, т. е. такое, при котором срабатывает компаратор, составляет 100 мВ. В соответствии с технической документацией для этого порога считывания скорость темнового счета при температуре (25 ± 10) °С составляет примерно 100 Гц. То есть с учетом мертвого времени порядка микросекунды [6] кремниевый фотоумножитель регистрирует до 100 темновых импульсов в секунду. Эти случайные импульсы могут лежать в другом спектральном диапазоне, поэтому, согласно технической документации, эффективность их регистрации в 4 и более раз меньше. Вместе с тем, учитывая возможное изменение коэффициента усиления за счет изменения напряжения (почти в 3 раза) или температуры (на 10 %), возможно их усиление до уровня основного сигнала, что приведет к изменению соотношения 0 и 1. Как отмечалось выше, для криптографических целей бинарный тест должен выполняться с точностью 6 бит из 10^6. Последовательность такой длины считывается с генератора более 15 мин. То есть стабильность напряжения и температуры должна быть такой, чтобы обеспечить эту точность в течение времени считывания. Таким образом, нестабильность случайной последовательности, тестируемой для криптографических целей, объясняется возможностью усиления темновых импульсов и нестабильностью температуры в процессе работы генератора.

Вывод

Проанализирована точность последовательности случайных чисел, необходимая для прохождения тестов на случайность для криптографических целей. Полученные результаты применены для объяснения нестабильности тестов, выдаваемых генератором случайных чисел, на основе излучения и детектирования фотонов. Оценена возможность использования кремниевых фотоумножителей в генераторах случайных чисел для криптографических целей.

Список литературы

1. Bernstein, D. J. Post-Quantum Cryptography / D. J. Bernstein, T. Lange // Nature. 2017. Vol. 13, No 549. P. 188–194. DOI: 10.1038/nature23461.
2. Пикуза, М. О. Оптимизация режимов работы генераторов случайных чисел / М. О. Пикуза, С. Ю. Михневич // Проблемы инфокоммуникаций. 2022. Т. 2, № 16. С. 46–51.
3. Herrero-Collantes, M. Quantum Random Number Generators / M. Herrero-Collantes, J. C. Garcia-Escartin // Reviews of Modern Physics. 2017. Vol. 89, No 1. https://doi.org/10.1103/RevModPhys.89.015004.
4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin [et al.]. Gaithersburg: National Institute of Standards and Technology. 2010. 131 p.
5. Carnahan, L. J. Security Requirements for Cryptographic Modules / L. J. Carnahan, M. E. Smid. Gaithersburg: National Institute of Standards and Technology, 1994.
6. Барановский, О. К. Исследование возможности использования лавинных фотодиодов в режиме одноквантовой регистрации для создания квантовых генераторов случайных чисел / О. К. Барановский, О. Ю. Горбадей, А. О. Зеневич // Приборы и техника эксперимента. 2018. № 1. С. 34–38. DOI: 10.7868/S0032816218010147.
7. Асаенок, М. А. Исследование возможности использования кремниевых фотоэлектронных умножителей для создания генераторов случайных числовых последовательностей / М. А. Асаенок, А. О. Зеневич, Е. В. Новиков // Известия вузов. Электроника. 2020. Т. 25, № 2. С. 114–122. DOI: 10.24151/1561-5405-2020-25-2-114-122.
8. Гулаков, И. Р. Влияние температуры на одноквантовые характеристики лавинных фотоприемников / И. Р. Гулаков, В. Л. Козлов, А. О. Зеневич // Доклады БГУИР. 2004. № 4. С. 21–25.
9. Асаенок, М. А. Коэффициент усиления кремниевого фотоэлектронного умножителя с низким напряжением питания / М. А. Асаенок, О. Ю. Горбадей, А. О. Зеневич // Проблемы инфокоммуникаций. 2017. № 2. С. 82–87.
10. Асаенок, М. А. Температурные характеристики кремниевых фотоэлектронных умножителей / М. А. Асаенок, О. Ю. Горбадей, А. О. Зеневич // Доклады БГУИР. 2018. № 2. С. 54–58.
11. Асаенок, М. А. Исследование характеристик кремниевых фотоэлектронных умножителей / М. А. Асаенок, А. О. Зеневич // Прикладная физика. 2018. № 6. С. 49–53.
12. Асаенок, М. А. Исследование амплитудных характеристик кремниевых фотоэлектронных умножителей / М. А. Асаенок, А. О. Зеневич, Е. В. Новиков // Прикладная физика. 2019. № 6. С. 97.

References

1. Bernstein D. J., Lange T. (2017) Post-Quantum Cryptography. *Nature*. 13 (549), 188–194. Doi: 10.1038/nature23461.
2. Pikuza M. O., Mikhnevich S. Yu. (2022) Operating Modes Optimization of Random Number Generators. *Problems of Infocommunications*. 2 (16), 46–51 (in Russian).
3. Herrero-Collantes M., Garcia-Escartin J. C. (2017) Quantum Random Number Generators. *Reviews of Modern Physics.* 89 (1). https://doi.org/10.1103/RevModPhys.89.015004.
4. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Hecket A., Dray J., San Vo (2010) *A Statistical Test Suitefor Random and Pseudorandom Number Generators for Cryptographic Applications.* Gaithersburg, National Institute of Standards and Technology Publ. 131.
5. Carnahan L. J., Smid M. E. (1994) *Security Requirements for Cryptographic Modules*. Gaithersburg, National Institute of Standards and Technology Publ.
6. Baranovsky O. K., Gorbadei O. Yu., Zenevich A. O. (2018) Investigation of the Possibility and Use of Avalanche Photodiodes in the Mode of Single-Quantum Registration for the Creation of Quantum Random Number Generators. *Instruments and Technique of Experiment*. (1), 34–38. DOI: 10.7868/S0032816218010147 (in Russian).
7. Asayonok M. A., Zenevich A. O., Novikov E. V. (2020) Study of the Possibility of Using Silicon Photoelectronic Multipliers to Create Generators of Random Numerical Sequences. *University News. Electronics*. 25 (2), 114–122. DOI: 10.24151/1561-5405-2020-25-2-114-122 (in Russian).
8. Gulakov I. R., Kozlov V. L., Zenevich A. O. (2004) Influence of Temperature on Single-Quantum Characteristics of Avalanche Photodetectors. *Doklady BGUIR*. (4), 21–25 (in Russian).
9. Asayonok M. A., Gorbadei O. Yu., Zenevich A. O. (2017) Low Voltage Silicon Photomultiplier Gain. *Problems of Infocommunications*. 2 (6), 82–87 (in Russian).
10. Asayonok M. A., Gorbadei O. Yu., Zenevich A. O. (2018) Temperature Characteristics of Silicon Photomultipliers. *Doklady BGUIR*. (2), 54–58 (in Russian).

11. Asayonok M. A., Zenevich A. O. (2018) Study of the Characteristics of Silicon Photomultipliers. *Applied Physics*. (6), 49–53 (in Russian).
12. Asayonok M. A., Zenevich A. O., Novikov E. V. (2019) Investigation of the Amplitude Characteristics of Silicon Photomultipliers. *Applied Physics.* (6), 96–101 (in Russian).

Вклад авторов

Пикуза М. О. осуществил экспериментальные измерения.
Пикуза М. О., Михневич С. Ю. провели теоретический расчет.
Михневич С. Ю., Сенкевич А. Ю. обосновали и описали результаты.

Authors' contribution

Pikuza M. O. made experimental measurements.
Pikuza M. O., Mikhnevich S.Yu. carried out a theoretical calculation.
Mikhnevich S. Yu., Siankevich A. Yu. substantiated and described the results.

Сведения об авторах

Пикуза М. О., аспирант кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники, инженер тематического отдела ОАО «КБ Радар» – управляющая компания холдинга «Системы радиолокации»

Михневич С. Ю., к. ф.-м. н., доцент, заведующая кафедрой инфокоммуникационных технологий Белорусской государственной академии связи

Сенкевич А. Ю., лаборант кафедры инфокоммуникационных технологий Белорусской государственной академии связи

Адрес для корреспонденции

220062, Республика Беларусь,
г. Минск, просп. Независимости, 117а
ОАО «КБ Радар» – управляющая компания
холдинга «Системы радиолокации»
Тел.: +375 33 650-31-78
E-mail: maksimpikuza@gmail.com
Пикуза Максим Олегович

Information about the authors

Pikuza M. O., Postgraduate at the Department of Information Radiotechnologies of the Belarusian State University of Informatics and Radioelectronics, Engineer at the Thematic Department of JSC "KB Radar" – Managing Director Holding Company of "Radar Systems"

Mikhnevich S. Yu., Cand. of Sci., Associate Professor, Head of the Department of Infocommunication Technologies of the Belarusian State Academy of Communications

Siankevich A. Yu., Laboratory Assistant at the Department of Infocommunication Technologies of the Belarusian State Academy of Communications

Address for correspondence

220062, Republic of Belarus,
Minsk, Nezavisimosti Ave., 117a
JSC "KB Radar" – Managing Director
Holding Company of "Radar Systems"
Tel.: +375 33 650-31-78
E-mail: maksimpikuza@gmail.com
Pikuza Maksim Olegovich