НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2018 Том 18 № 6 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2018 Vol. 18 No 6 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.421.5

АНАЛИЗ ЭНТРОПИИ ПОКАЗАНИЙ ИНЕРЦИАЛЬНОГО МОДУЛЯ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ ПРИ ОТСУТСТВИИ ВНЕШНИХ ВОЗМУЩЕНИЙ

И.А. Авдонин[a], М.Б. Будько[a], М.Ю. Будько[a], А.В. Гирик[a], В.А. Грозов[a], Д.С. Ярошевский[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: dimonyarosh@mail.ru

Информация о статье
Поступила в редакцию 28.08.18, принята к печати 18.10.18
doi: 10.17586/2226-1494-2018-18-6-1054-1059
Язык статьи – русский

Ссылка для цитирования: Авдонин И.А., Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А., Ярошевский Д.С. Анализ энтропии показаний инерциального модуля киберфизической системы при отсутствии внешних возмущений // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1054–1059. doi: 10.17586/2226-1494-2018-18-6-1054-1059

Аннотация

Предмет исследования. Исследованы киберфизические системы, находящие широкое применение в различных сферах человеческой деятельности. Проанализирована информационная безопасность каналов связи, используемых такими системами. Общепринятый метод решения этой задачи – криптографическая защита данных, основанная на использовании случайных последовательностей. Надежность подобных криптосистем определяется качеством используемых случайных последовательностей. По этой причине предпочтительно применять истинно случайные последовательности. Получение истинно случайных последовательностей требует наличия источников энтропии физической природы. Целью настоящей работы является исследование методов получения случайных чисел в киберфизических системах с использованием инерциальных датчиков, находящихся в составе киберфизических систем. **Метод.** Проведена оценка качества битовой последовательности, сформированной из показаний датчиков, путем определения статистических свойств случайной последовательности. **Основные результаты**. Согласно результатам исследования, показания датчиков пространственного положения, использующихся в инерциальных измерительных модулях киберфизических систем, в состоянии покоя обладают невысокой энтропией, и для их применения в качестве источника для генерации случайных последовательностей необходима дополнительная постобработка. **Практическая значимость**. Результаты исследования могут быть использованы для получения киберфизическими системами случайных последовательностей без применения дополнительных устройств при наличии в их составе датчиков инерциальных систем. В дальнейшем планируется считывание показаний с датчиков во время перемещения, в частности беспилотного летательного аппарата, применение экстракторов и методов, которые позволят улучшить характеристики битовой последовательности.

Ключевые слова
киберфизическая система, истинно случайные последовательности, случайные числа, инерциальные датчики, источник энтропии

ENTROPY ANALYSIS OF DATA COLLECTED FROM INERTIAL MEASUREMENT UNIT OF CYBER-PHYSICAL SYSTEM UNDER NON-DISTURBED CONDITIONS

I.A. Avdonin[a], M.B. Budko[a], M.Yu. Budko[a], A.V. Guirik[a], V.A. Grozov[a], D.S. Iaroshevskii[a]

[a]ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: dimonyarosh@mail.ru

Article info
Received 28.08.18, accepted 18.10.18
doi: 10.17586/2226-1494-2018-18-6-1054-1059
Article in Russian

For citation: Avdonin I.A., Budko M.B., Budko M.Yu., Guirik A.V., Grozov V.A., Iaroshevskii D.S. Entropy analysis of data collected from inertial measurement unit of cyber-physical system under non-disturbed conditions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1054–1059 (in Russian). doi: 10.17586/2226-1494-2018-18-6-1054-1059.

Abstract

Subject of Research. Nowadays cyber-physical systems are widely used for many purposes. We consider the provision of

information security of data channels in such systems. Cryptographic data security approach based on random sequences is commonly used to solve this task. Its reliability depends on quality of random data being used, thus truly random sequences are preferable for application. Truly random data generation is a time-consuming process and it requires entropy sources of physical nature. The goal of the paper presented is to research methods and approaches of collecting random numbers using inertial measurement unit as a part of cyber-physical system. **Method.** Quality assessment of a binary sequence was carried out during the research by determination of random sequence statistical characteristics. **Main Results.** Research results have shown up that raw data collected from onboard inertial sensors possess lack of entropy under non-disturbed conditions, therefore an additional post-processing is required. **Practical Relevance.** The results of the research can be used to obtain random sequences for on board cyber-physical systems equipped with inertial measurement units without the use of additional devices. It is planned to collect data from a flying unmanned aerial system in future to apply extractors and to utilize other methods in order to improve quality of a binary sequence.

Keywords
cyber-physical system, truly random sequences, random numbers, inertial sensors, entropy source

Введение

Киберфизические системы (КФС) все активнее применяются в различных сферах человеческой деятельности. Такие системы широко используют обмен данными в режиме реального времени, что делает актуальным обеспечение информационной безопасности для используемых каналов связи [1]. Общепринятым методом решения этой задачи является криптографическая защита данных. Технологии криптозащиты часто базируются на использовании случайных последовательностей. Различают истинно случайные и псевдослучайные последовательности. Надежность криптосистем во многом определяется качеством применяемых случайных последовательностей, поэтому предпочтительным является применение истинно случайных последовательностей (ИСП). В настоящее время источником случайных чисел (СЧ) в КФС, как правило, являются криптостойкие алгоритмы генерации СЧ. Однако в некоторых случаях, когда предъявляются особые требования к информационной безопасности, необходимо использовать истинно СЧ, в том числе в качестве ключа или инициализирующей последовательности для криптостойких алгоритмов [2].

Традиционными способами получения СЧ являются генераторы, основанные на атмосферных шумах, на статических ячейках памяти с произвольным доступом [3], квантовые генераторы и др. [4]. Их применение в КФС осложнено необходимостью использования дополнительного оборудования. Современные КФС часто включают в себя инерциальные датчики, которые могут рассматриваться в качестве возможных источников ИСП [5–9]. Целью настоящей работы является исследование методов получения СЧ в КФС с использованием инерциальных датчиков, находящихся в составе этих систем.

В работе [10] применялся модуль на основе MPU9250. Битовая последовательность была сформирована из данных акселерометра, гироскопа и магнитометра путем применения сложной схемы экстракции значений. Сначала 16 бит преобразуются в 9 десятичных значений, потом в 9 двоичных разрядов; на третьем шаге применяется экстрактор [11, 12]. Предлагается исследовать датчики отдельно друг от друга, так как многие КФС содержат в своем составе только один датчик. Также исключение первого и второго шагов при экстракции значений позволяет упростить и ускорить постобработку значений.

Состав инерциальных датчиков КФС

Инерциальные датчики в КФС представляют собой микроэлектромеханические системы (МЭМС), обычно состоящие из акселерометра и гироскопа. Также встречаются варианты использования только акселерометра или гироскопа. Инерциальные датчики имеют различную чувствительность: некоторые – фиксированную, некоторые – настраиваемую. Получение показаний с МЭМС-датчиков может осуществляться путем считывания аналогового сигнала и последующего его преобразования для датчиков, поддерживающих только аналоговый выход. Для датчиков, имеющих интегрированную электронику обработки сигнала, обмен информацией может происходить по интерфейсам Inter-Integrated Circuit (I^2C) или Serial Peripheral Interface (SPI). Показания МЭМС-датчиков содержат случайные компоненты, которые меняются непредсказуемым образом и могут служить источником случайности. Однако, как показывает практика, данные от физических источников содержат отклонения и корреляции из-за систематических ошибок при измерениях или неслучайных составляющих. Для устранения этих недостатков требуется постобработка полученных последовательностей [13].

В исследовании использовался МЭМС-датчик MPU9250 компании InvenSense [14], входящий в состав модуля управления и навигации мультироторным беспилотным летательным аппаратом (БПЛА) [15]. MPU9250 – это девятиосевой сенсор движения, состоящий из трехосевых акселерометра, гироскопа и магнитометра. Считывание показаний датчика осуществлялось с использованием интерфейса I^2C (скорость считывания до 400 кбит/с), также возможно использование шины SPI (скорость считывания до 20 Мбит/с).

Опишем подробнее характеристики акселерометра и гироскопа, входящих в состав MPU9250. В табл. 1 приведены пределы измеряемых значений и чувствительности этих датчиков, где g – ускорение

свободного падения на поверхности Земли. Размер значимых показаний, считываемых с акселерометра и гироскопа, 16 бит. Частота считывания показаний с датчиков ограничивается пропускной способностью используемого интерфейса и частотой обновления регистров акселерометра и гироскопа MPU9250 (4 кГц для акселерометра и 8 кГц – для гироскопа). При считывании показаний с частотой 4 кГц поток данных с датчиков составляет 375 кбит/с.

Акселерометр		Гироскоп	
пределы измеряемых значений, *g*	чувствительность, LSB/*g*	пределы измеряемых значений, ...°/с	чувствительность, LSB/°/с
±2	±16,384	±250	±131
±4	±8,192	±500	±65,5
±8	±4,096	±1000	±32,8
±16	±2,048	±2000	±16,4

Таблица 1. Характеристики акселерометра и гироскопа, входящих в состав MPU9250

Исследовалась возможность использования показаний инерциального измерительного модуля КФС в качестве исходных данных для формирования последовательности СЧ. Для этого необходимо было считать и обработать показания датчиков, сформировать битовую последовательность из полученных данных и оценить ее качество путем определения статистических свойств случайной последовательности.

Исследуемые параметры битовых последовательностей

Истинно случайные последовательности – это случайные числа, представленные в виде последовательности. СЧ являются реализациями некоторой случайной величины (СВ). В свою очередь, СВ определяется как функция пространства элементарных событий, принимающая вещественные значения с некоторыми вероятностями. ИСП, таким образом, представима как последовательность статистически не зависящих друг от друга величин, принимающих одно из множества непредсказуемых значений. ИСП также характеризуется отсутствием периодичности и имеет равномерное распределение.

В качестве параметров битовой последовательности использовались среднеквадратическое отклонение (СКО), минимальная энтропия $E_{\min}$, параметр k, позволяющий оценить отношение энтропии к разрядности чисел содержащихся в последовательности, и математическое ожидание μ.

Минимальная энтропия [16] заданного распределения X на $\{0, 1\}^n$ определяется формулой

$$E_{\min}(X) = \min_{x\in\{0,1\}^n} \log_2 \frac{1}{\Pr[X = x]}. \quad (1)$$

Если для распределения X $E_{\min}=m$, то вероятность появления какого-либо одного элемента x из X не превосходит $1/2^m$ для всех $x \in X$. Минимальная энтропия является важной характеристикой распределения, фиксирующей количество случайности, которое способно поддерживать распределение. Несмотря на то что элементы X имеют разрядность n бит, из-за смещения распределения X не может содержать достаточную энтропию, чтобы поддерживать извлечение n несмещенных бит. Только m бит случайны и могут быть получены из распределения, которое имеет энтропию m, независимо от длины элемента распределения n.

В связи с тем, что значение минимальной энтропии связано с разрядностью исходных данных, введем параметр:

$$k = \frac{E_{\min}(X)}{n}, \quad (2)$$

где n – разрядность элемента последовательности

Сбор данных при отсутствии внешних возмущений

Сбор данных осуществлялся, когда БПЛА находился на горизонтальной поверхности в состоянии покоя, внешние возмущения на датчик отсутствовали. Для каждого варианта настройки чувствительности датчика и частоты считывания показаний были взяты выборки объемом 900 000 значений по каждой из осей датчика.

В табл. 2 представлены результаты исследования последовательностей, сформированных из 16-битных значений по каждой из осей датчиков и путем применения экстрактора

$$e = xy + z, \quad (3)$$

где x – координата по оси X; y – координата по оси Y; z – координата по оси Z.

Такой экстрактор применялся в работах [11, 12] для улучшения характеристик битовой последовательности.

СКО данных после применения экстрактора вычислено экспериментально, так же как и по каждой из осей датчика.

Чувствительность датчика (при частоте считывания данных, Гц)	Параметр	Ось X	Ось Y	Ось Z	e
Источник данных – акселерометр					
±2,048 LSB/g (3000)	μ	–461,59	275,42	–17361,5	–144450,79
	СКО	39,41	40,75	58,76	21525,51
	E_{min}	4,64	4,62	5,18	12,3
	k	0,29	0,29	0,32	0,38
±16,384 LSB/g (3000)	μ	–502,02	33,83	–17365,1	–34343,60
	СКО	44,62	25,68	127,1	12286,57
	E_{min}	4,63	3,72	5,3	10,59
	k	0,29	0,23	0,33	0,33
Источник данных – гироскоп					
±32,8 LSB/°/с (3000)	μ	–7,99	3,49	–6,89	–40,10
	СКО	5,63	9,92	4,53	3079,88
	E_{min}	3,42	3,67	3,47	6,33
	k	0,21	0,23	0,22	0,4
±32,8 LSB/°/с (1000)	μ	–8,19	3,74	–7,21	–39,74
	СКО	4,63	5,53	4,47	62,63
	E_{min}	3,44	3,65	3,47	6,38
	k	0,21	0,23	0,22	0,4

Таблица 2. Результаты исследования последовательностей (n = 16 бит), сформированных из данных датчиков БПЛА, находящегося в состоянии покоя

На рис. 1 представлен график распределения частот для оси Z акселерометра. Первичные данные, считываемые с осей акселерометра, не имеют размерности и представлены на графике в условных единицах.

Рис. 1. График распределения частот для оси Z акселерометра при отсутствии внешних возмущений (16 бит, k = 0,32)

В табл. 3 представлены результаты исследования последовательностей, сформированных путем отбрасывания части старших бит и применением экстрактора (3).

Чувствительность датчика (при частоте считывания данных, Гц)	Параметр	Ось X (8 бит)	Ось Y (8 бит)	Ось Z (8 бит)	e
Источник данных – акселерометр					
±2,048 LSB/g (3000)	μ	74,18	93,14	99,07	7005,45
	СКО	60,92	88,90	74,53	10383,04
	E_{min}	4,64	4,62	5,18	9,27
	k	0,58	0,58	0,65	0,58
±16,384 LSB/g (3000)	μ	107,88	33,77	103,45	3746,34
	СКО	96,16	5,24	76,64	3333,66
	E_{min}	4,63	3,72	5,27	9,27
	k	0,58	0,47	0,66	0,58
Источник данных – гироскоп					
±32,8 LSB/°/с (3000)	μ	236,43	59,04	230,06	14028,54
	СКО	51,24	101,69	64,88	24674,12
	E_{min}	3,42	3,67	3,47	6,99
	k	0,43	0,46	0,43	0,44
±32,8 LSB/°/с (1000)	μ	236,69	54,82	232,01	12987,14
	СКО	50,12	98,66	61,18	23857,52
	E_{min}	3,44	3,65	3,47	7,04
	k	0,43	0,46	0,43	0,44

Таблица 3. Результаты исследования последовательностей (n = 8 бит), сформированных из данных датчиков БПЛА, находящегося в состоянии покоя

На рис. 2 представлен график распределения частот для оси *Z* акселерометра после отбрасывания 8 старших бит.

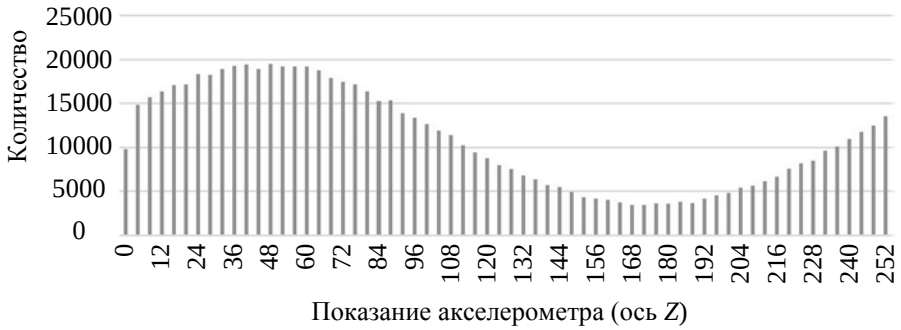

Рис. 2. График распределения частот для оси *Z* акселерометра при отсутствии внешних возмущений (8 младших бит, k = 0,66)

В табл. 4 представлены результаты исследования последовательностей, сформированных путем применения операции побитовой конкатенации с использованием показаний трех осей акселерометра.

Чувствительность датчика, LSB/*g*	Частота считывания данных, Гц	Параметр	Побитовая конкатенация
±2,048	3000	μ	2145792571,01
		СКО	1240481261,48
		E_{min}	17,98
		k	0,37

Таблица 4. Результаты исследования последовательностей, сформированных путем применения операции побитовой конкатенации с использованием показаний трех осей акселерометра (n = 48 бит)

Заключение

Анализ полученных результатов показал, что применение экстрактора одновременно с увеличением разрядности данных не приводит к значительному улучшению битовой последовательности. Изменение чувствительности датчиков и частоты получения с них данных не оказывает заметного влияния на параметры битовой последовательности. Кроме того, в процессе исследования было определено, что показания акселерометра обладают на 30–40 % большей минимальной энтропией, чем показания гироскопа. Отбрасывание части старших битов приводит к увеличению параметра k в два раза, что свидетельствует о повышении минимальной энтропии относительно разрядности числа. Это объясняется тем, что датчики находятся в состоянии покоя, и внешние случайные воздействия оказывают влияние только на младшие восемь разрядов, даже при максимальных настройках чувствительности.

В дальнейшем планируется применение других экстракторов и методов, которые позволят улучшить характеристики битовой последовательности. По результатам исследования было определено, что показания датчиков пространственного положения, использующихся в инерциальных измерительных модулях киберфизических систем, в состоянии покоя обладают невысокой энтропией, и для их применения в качестве источника для генерации случайных последовательностей необходима дополнительная постобработка. Также планируется использование тестов NIST для анализа случайности битовой последовательности.

Литература

1. Lo Re G., Milazzo F., Ortolani M. Secure random number generation in wireless sensor networks // Concurrency Computation: Practice and Experience. 2015. V. 27. N 15. P. 3842–3862. doi: 10.1002/cpe.3311
2. Avdonin I., Budko M., Budko M., Grozov V., Guirik A. A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads // Proc. 9th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2017. P. 410–413. doi: 10.1109/icumt.2017.8255167
3. Van Herrewege A., van der Leest V., Schaller A., Katzenbeisser S., Verbauwhede I. Secure PRNG seeding on commercial off-the-shelf microcontrollers // Proc. TrustED'13. Berlin, 2013. P. 55–64. doi: 10.1145/2517300.2517306
4. Pawlowski M.P., Jara A., Ogorzalek M. Harvesting entropy

References

1. Lo Re G., Milazzo F., Ortolani M. Secure random number generation in wireless sensor networks. *Concurrency Computation: Practice and Experience*, 2015, vol. 27, no. 15, pp. 3842–3862. doi: 10.1002/cpe.3311
2. Avdonin I., Budko M., Budko M., Grozov V., Guirik A. A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads. *Proc. 9th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT*, 2017, pp. 410–413. doi: 10.1109/icumt.2017.8255167
3. Van Herrewege A., van der Leest V., Schaller A., Katzenbeisser S., Verbauwhede I. Secure PRNG seeding on commercial off-the-shelf microcontrollers. *Proc. TrustED'13*. Berlin, 2013, pp. 55–64. doi: 10.1145/2517300.2517306
4. Pawlowski M.P., Jara A., Ogorzalek M. Harvesting entropy for random number generation for Internet of Things constrained

for random number generation for Internet of Things constrained devices using on-board sensors // Sensors. 2015. V. 15. N 10. P. 26838–26865. doi: 10.3390/s151026838
5. Loutfi J., Chehab A., Elhajj I.H., Kayssi A. Smartphone sensors as random bit generators // IEEE/ACS 11th Int. Conf. on Computer Systems and Applications. 2015. P. 773–780. doi: 10.1109/AICCSA.2014.7073279
6. Wallace K., Moran K., Novak E., Zhou G., Sun K. Toward sensor-based random number generation for mobile and IoT devices // IEEE Internet of Things Journal. 2015. V. 3. N 6. doi: 10.1109/JIOT.2016.2572638
7. Bouda J., Krhovjak J., Matyas V., Svenda P. Towards true random number generation in mobile environments // Lecture Notes in Computer Science. 2009. V. 5838. P. 179–189. doi: 10.1007/978-3-642-04766-4_13
8. Hennebert C., Hossayni H., Lauradoux C. Entropy harvesting from physical sensors // Proc. 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'13). Budapest, Hungary, 2013. P. 149–154. doi: 10.1145/2462096.2462122
9. Смагин А.А., Клочков А.Е., Григорьев А.Ю. Исследование возможности использования датчиков мобильных устройств для генерации случайных последовательностей // Автоматизация процессов управления. 2017. № 3. С. 103–109.
10. Bedekar N., Shee C. A novel approach to true random number generation in wearable computing environments using MEMS sensors // Lecture Notes in Computer Science. 2014. V. 8957. P. 530–546. doi: 10.1007/978-3-319-16745-9_29
11. Barak B., Impagliazzo R., Wigderson A. Extracting randomness using few independent sources // Proc. 45th Annual IEEE Symposium on Foundations of Computer Science. 2004. P. 384–393. doi: 10.1109/focs.2004.29
12. Barak B., Shaltiel R., Tomer E. True random number generators secure in a changing environment // Lecture Notes in Computer Science. 2003. P. 166–180. doi: 10.1007/978-3-540-45238-6_14
13. Hong S.L., Liu C. Sensor-based random number generator seeding // IEEE Access. 2015. V. 3. P. 562–568. doi: 10.1109/ACCESS.2015.2432140
14. MPU9250 product specification. InvenSense Inc., 2016. 42 p.
15. Беляев С.С., Будько М.Б., Будько М.Ю., Гирик А.В., Жигулин Г.П. Функциональное проектирование модуля управления и навигации мультироторным БПЛА // Радиопромышленность. 2015. № 4. С. 77–87.
16. Voris J., Saxena N., Halevi T. Accelerometers and randomness: perfect together // Proc. 4th ACM Conference on Wireless Network Security (WISEC 2011). Hamburg, Germany, 2011. P. 115–126. doi: 10.1145/1998412.1998433

devices using on-board sensors. *Sensors*, 2015, vol. 15, no. 10, pp. 26838–26865. doi: 10.3390/s151026838
5. Loutfi J., Chehab A., Elhajj I.H., Kayssi A. Smartphone sensors as random bit generators. *IEEE/ACS 11th Int. Conf. on Computer Systems and Applications*, 2015, pp. 773–780. doi: 10.1109/AICCSA.2014.7073279
6. Wallace K., Moran K., Novak E., Zhou G., Sun K. Toward sensor-based random number generation for mobile and IoT devices. *IEEE Internet of Things Journal*, 2015, vol. 3, no. 6. doi: 10.1109/JIOT.2016.2572638
7. Bouda J., Krhovjak J., Matyas V., Svenda P. Towards true random number generation in mobile environments. *Lecture Notes in Computer Science*, 2009, vol. 5838, pp. 179–189. doi: 10.1007/978-3-642-04766-4_13
8. Hennebert C., Hossayni H., Lauradoux C. Entropy harvesting from physical sensors. *Proc. 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC'13*. Budapest, Hungary, 2013, pp. 149–154. doi: 10.1145/2462096.2462122
9. Smagin A.A., Klochkov A.E., Grigor'ev A.Yu. Researching the ability of using mobile device sensors for generation of random sequencies. *Automation of Control Processes*, 2017, no. 3, pp. 103–109. (in Russian)
10. Bedekar N., Shee C. A novel approach to true random number generation in wearable computing environments using MEMS sensors. *Lecture Notes in Computer Science*, 2014, vol. 8957, pp. 530–546. doi: 10.1007/978-3-319-16745-9_29
11. Barak B., Impagliazzo R., Wigderson A. Extracting randomness using few independent sources. *Proc. 45th Annual IEEE Symposium on Foundations of Computer Science*, 2004, pp. 384–393. doi: 10.1109/focs.2004.29
12. Barak B., Shaltiel R., Tomer E. True random number generators secure in a changing environment. *Lecture Notes in Computer Science*, 2003, pp. 166–180. doi: 10.1007/978-3-540-45238-6_14
13. Hong S.L., Liu C. Sensor-based random number generator seeding. *IEEE Access*, 2015, vol. 3, pp. 562–568. doi: 10.1109/ACCESS.2015.2432140
14. *MPU9250 product specification*. InvenSense Inc., 2016, 42 p.
15. Belyaev S.S., Budko M.B., Budko M.Y., Guirik A.V., Zhigulin G.P. Functional design of flight and navigation controller unit for multirotor unmanned aerial vehicle. *Radio Industry*, 2015, no. 4, pp. 77–87. (in Russian)
16. Voris J., Saxena N., Halevi T. Accelerometers and randomness: perfect together. *Proc. 4th ACM Conference on Wireless Network Security, WISEC 2011*. Hamburg, Germany, 2011, pp. 115–126. doi: 10.1145/1998412.1998433

Авторы

Авдонин Иван Александрович – инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-1131-0202, avdoninivan@mail.ru

Будько Марина Борисовна – кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57192541740, ORCID ID: 0000-0001-7054-5709, mbbudko@corp.ifmo.ru

Будько Михаил Юрьевич – кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57192541739, ORCID ID: 0000-0002-1444-277X, mbudko@corp.ifmo.ru

Гирик Алексей Валерьевич – кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57192558077, ORCID ID: 0000-0002-4021-7605, avg@corp.ifmo.ru

Грозов Владимир Андреевич – инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-7998-8175, vladimirgrozov@mail.ru

Ярошевский Дмитрий Сергеевич – техник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0001-9269-3075, dimonyarosh@mail.ru

Authors

Ivan A. Avdonin – engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-1131-0202, avdoninivan@mail.ru

Marina B. Budko – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57192541740, ORCID ID: 0000-0001-7054-5709, mbbudko@corp.ifmo.ru

Mikhail Yu. Budko – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57192541739, ORCID ID: 0000-0002-1444-277X, mbudko@corp.ifmo.ru

Alexey V. Guirik – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57192558077, ORCID ID: 0000-0002-4021-7605, avg@corp.ifmo.ru

Vladimir A. Grozov – engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-7998-8175, vladimirgrozov@mail.ru

Dmitry S. Iaroshevskii – technician, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0001-9269-3075, dimonyarosh@mail.ru