УДК 004.421.5

А.А. Смагин, А.Е. Клочков, А.Ю. Григорьев

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАТЧИКОВ МОБИЛЬНЫХ УСТРОЙСТВ ДЛЯ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Смагин Алексей Аркадьевич, *доктор технических наук, профессор, окончил радиотехнический факультет Ульяновского политехнического института. Заведующий кафедрой «Телекоммуникационные технологии и сети» Ульяновского государственного университета. Имеет статьи, изобретения, монографии в области разработки информационных систем различного назначения. [e-mail: smaginaa1@mail.ru].*

Клочков Андрей Евгеньевич, *окончил факультет математики и информационных технологий УлГУ, старший преподаватель кафедры «Информационная безопасность и теория управления» УлГУ. Имеет опыт работы в области защиты информации от утечки по техническим каналам связи. [e-mail: ak@ulsu.ru].*

Григорьев Александр Юрьевич, *окончил факультет математики и информационных технологий УлГУ, аспирант кафедры «Телекоммуникационные технологии и сети» УлГУ. Инженер-программист ФНПЦ АО «НПО «Марс». Имеет работы в области статистического тестирования случайных последовательностей. [e-mail: als73@mail.ru].*

Аннотация

В настоящей работе исследуется возможность применения датчиков положения в пространстве для генерации случайных последовательностей бит, применяемых в криптографии. В работе для создания аппаратного генератора используются датчики акселерометр и гироскоп, установленные на трёх мобильных устройствах. Источником случайности является постоянное изменение показаний датчиков за счёт перемещения устройства в пространстве, его незначительных колебаний и вибраций в процессе эксплуатации. Предлагаются способы обработки показаний датчиков для формирования последовательностей бит. Рассмотрены этапы тестирования и критерий подтверждения случайности. Тестирование последовательностей на случайность проводится с помощью различных статистических тестов, входящих в программный пакет NIST STS. В статье приводятся экспериментальные результаты тестирования датчиков (акселерометр и гироскоп) трёх мобильных устройств.

Ключевые слова: акселерометр, гироскоп, генератор случайных чисел, статистические тесты, NIST STS.

RESEARCHING THE ABILITY OF USING MOBILE DEVICE SENSORS FOR GENERATION OF RANDOM SEQUENCIES

Aleksei Arkadevich Smagin, *Doctor of Engineering, Professor; graduated from the Faculty of Radioengineering of Ulyanovsk Polytechnic Institute; Head of the Department of Telecommunications Technologies and Networks at Ulyanovsk State University; an author of articles, inventions, and monographs in the field of different-purpose information system development. e-mail: smaginaa1@mail.ru.*

Andrei Evgenevich Klochkov, *graduated from the Faculty of Mathematics and Information Technologies of Ulyanovsk State University, Senior Lecturer at the Department of Information Security and Management Theory of Ulyanovsk State University; experienced in of work in the field of information security from leakages through technical communication channels. e-mail: ak@ulsu.ru.*

Aleksandr Iurevich Grigorev, *graduated from the Faculty of Mathematics and Information Technologies of Ulyanovsk State University; Postgraduate Student at the Department of Telecommunication Technologies and Networks of Ulyanovsk State University; Software Engineer at Federal Research-and-Production Center Joint Stock Company 'Research-and-Production Association 'Mars'; an author of articles in the field of statistical testing of random sequences. e-mail: als73@mail.ru.*

Abstract

The article considers researches of ability of using digital position monitoring encoders for generation of bit random sequences used in cryptography. In order to create hardware generator, gyroscope and accelerometer sensors installed on three mobile devices are used. The source of randomness is the regular change of sensor data due to movement in space, minor fluctuations and vibrations of a device during operation. The article suggests the methods of position sensor data processing for creating bit sequences. The stages of testing and the criterion for confirmation of randomness are discussed. The NIST STS software package contains different statistical tests that are used for randomness testing of sequences. The article includes the results of the experiments of testing the sensors (accelerometer and gyroscope) of three mobile devices.

Key words: accelerometer, gyroscope, random numbers generator, statistical tests, NIST STS.

Введение

Широкое проникновение в различные сферы человеческой жизни современных смартфонов, планшетов и других мобильных устройств делает необходимым обеспечить высокий уровень информационной безопасности передаваемых данных, в том числе применение качественных систем шифрования информации. Для получения случайных последовательностей, применяемых в криптографии (ключи шифрования, одноразовые шифр-блокноты, случайные параметры криптографических алгоритмов [1]), используются программные и аппаратные генераторы.

Чтобы оценить качество генерируемых последовательностей используются различные статистические тесты. Для проверки на случайность специально разработаны пакеты статистических тестов, содержащие различные алгоритмы проверки. Среди них наиболее распространены тесты NIST STS, DIEHARD, CRYPT-X и т. д.

Мобильные устройства снабжены различными датчиками, облегчающими взаимодействие с пользователем. Больше всего распространены встроенные датчики ориентации в пространстве (акселерометр и гироскоп), регистрирующие изменения положения в пространстве. В данной работе предлагается использовать показания датчиков ориентации в качестве источника энтропии для получения случайных последовательностей, а для оценки их качества применяется свободно распространяемый пакет статистических тестов NIST STS [2].

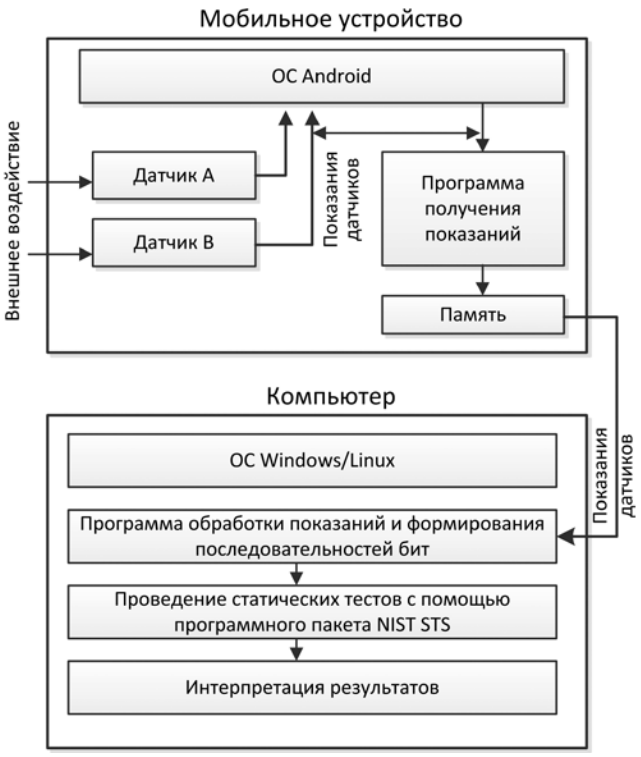

Рис. 1. Модель проведения исследования

Исследование включает следующие этапы:

а) Получение с датчиков показаний, которые будут являться источником для формирования последовательностей бит. Для снятия показаний разработан программный комплекс под ОС Android;

б) Обработка показаний, формирование битовых последовательностей;

в) Проведение статистических тестов для выявления случайных последовательностей;

г) Анализ и обработка полученных результатов тестирования.

На рисунке 1 представлена общая модель проведения исследования. На мобильное устройство оказывается некоторое внешнее воздействие (перемещение в пространстве, вращение и т. д.). Датчики непрерывно регистрируют изменение положения в пространстве. Программа получения показаний запрашивает данные с датчиков и сохраняет полученные показания в памяти устройства. Затем на компьютере собранные показания обрабатываются и различными способами формируются последовательности бит. Далее с помощью пакета статистических тестов NIST STS проводится анализ последовательностей бит. По результатам тестирования делается вывод о качестве сформированных последовательностей.

1 Датчики, используемые в исследовании

В настоящей работе использовалось несколько мобильных устройств под управлением ОС Android. В составе каждого из мобильных устройств имеются по два датчика: трехосные акселерометр и гироскоп [3].

Трехосный акселерометр – устройство, измеряющее разность между истинным ускорением объекта и гравитационным ускорением вдоль трёх осей. Он отслеживает ориентацию мобильного устройства относительно направления постоянно действующей силы гравитации Земли, а его показания – разность между значением ускорения вдоль оси X, Y или Z устройства

(направление осей представлено на рисунке 2) и силы гравитации Земли.

Трёхосный гироскоп – устройство, измеряющее изменения углов ориентации связанного с ним тела относительно инерциальной системы координат. В мобильных устройствах гироскоп измеряет угловую скорость V_x, V_y, V_z (рис. 2) относительно трёх осей X, Y и Z соответственно.

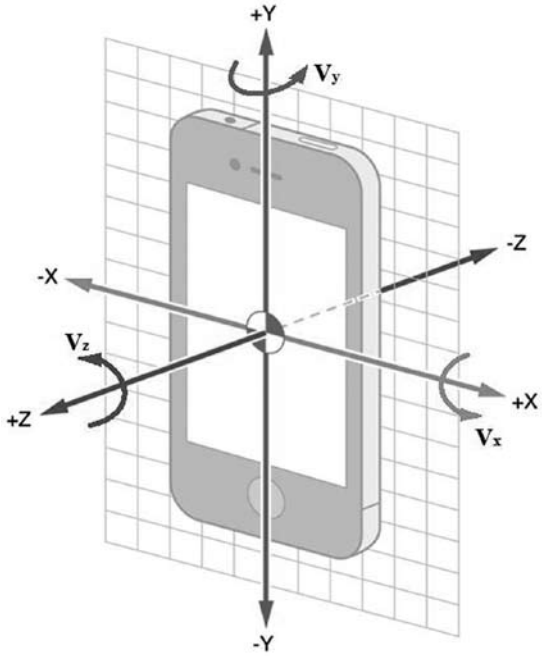

Рис. 2. Направление осей координат на мобильных устройствах

Все протестированные мобильные устройства были разбиты на группы. В группу № 1 вошли датчики планшета Digma iDx7, группа № 2 содержит датчики смартфона Sony ZR, группа № 3 – датчики смартфона Samsung Galaxy Note 2. Для обозначения датчика акселерометра используется литера «A», а для датчика гироскопа – литера «B». Например, датчик гироскопа из первой группы будет обозначаться 1B.

2 Получение и обработка показаний датчиков

Данные с датчиков испытуемых мобильных устройств снимались преимущественно в подвижном состоянии. Показания с каждой оси координат являются вещественными числами типа float (в соответствии со стандартом IEEE 754-2008 [4]). Полученные числа типа float представляют собой последовательность длиной 32 бита (рис. 3).

Формирование последовательностей выполняется следующим образом: из каждого показания берётся один i-й бит и добавляется в i-ю последовательность. Всего из набора показаний с датчика формируется 96 последовательностей бит: три оси координат по 32 бита показания на каждую. Затем каждая сформированная последовательность проходит статистические тесты из программного пакета NIST STS [2].

Перед тем как сформировать битовые последовательности, к полученным показаниям датчиков применяются два фильтра входных значений.

Фильтр 1. Для каждого датчика при неподвижном состоянии устройства находится размах показаний Δ – наибольшее расстояние между минимальным и максимальным значениями для трёх осей координат. Для этого вычисляется Δ_i ($i = 1, 2, 3$ соответственно для осей X, Y, Z) по формуле 1:

$$\Delta_i = |a\_max_i - a\_min_i|, \quad (1)$$

где a_min_i и a_max_i – минимальное и максимальное показание для i-й оси. Δ – наибольшее из значений Δ_i.

Далее для каждой оси координат обрабатывается набор показаний, полученный с датчика. Если разность между текущим и предыдущим используемым показанием меньше Δ, то текущее значение отбрасывается, иначе оно используется для формирования последовательности бит. Этот фильтр позволяет не рассматривать показания в пределах Δ, тем самым исключая обработку данных, полученных в неподвижном или малоподвижном состоянии (одинаковые или близкие по значению показания). В таблице 1 приведены вычисленные Δ для каждого датчика.

Таблица 1

Параметры Δ для датчиков

Датчик	Значение Δ
1A	0,152832 м/с^2
1B	0,0117275 рад/с
2A	0,536301 м/с^2
2B	0,006874 рад/с
3A	0,23942016 м/с^2
3B	0,0033597583 рад/с

Фильтр 2. В этом способе обработки для каждого возможного показания датчика d задан порядковый номер N. Его можно вычислить по формуле $N = d / \Delta d$, где Δd – шаг дискретизации (расстояние между ближайшими возможными показаниями датчиками).

Рис. 3. Представление числа типа float

Последовательность бит формируется из младшего бита порядкового номера N. Показания датчика B в области (−0,3; 0,3) встречаются наиболее часто и характерны для неподвижного и малоподвижного состоянии устройства. Поэтому при формировании последовательностей бит дополнительно отбрасывались показания из данной области.

При использовании в реальных условиях нужно учесть тот факт, что положение в пространстве мобильного устройства постоянно меняется. Поэтому требуется, чтобы последовательности, составленные из i-го бита ($i = 0, 1, \ldots, 31$, рис. 3) показания, проходили все тесты на случайность для всех осей координат.

3 Проведение тестов

Для проведения статистических тестов используется пакет NIST STS (The National Institute of Standards and Technology Statistical Test Suite). Он содержит 15 статистических тестов [2] (фактически их 188, так как некоторые выполняются несколько раз с различными параметрами), целью которых является определение меры случайности двоичных последовательностей, порождённых либо аппаратными, либо программными генераторами случайных чисел. Эти тесты основаны на различных статистических свойствах, присущих только случайным последовательностям.

При выполнении каждого статистического теста проверяется нулевая гипотеза H_0 о том, что исследуемая последовательность является случайной. Так же задаётся альтернативная гипотеза H_a, в соответствии с которой последовательность не случайна. Принимая гипотезу H_0, есть вероятность ошибиться α (вероятность совершить ошибку первого рода, также называется уровнем значимости [2]). В каждом тесте последовательность бит делится на подпоследовательности и вычисляются значения $p\text{-}value$ ($p\text{-}value$ принадлежит отрезку [0, 1]) – вероятность того, что идеальный генератор случайных чисел произвел бы последовательность менее случайную, чем исследуемая, для типа неслучайности, проверяемого тестом. Если $p\text{-}value < \alpha$ (в работе принята $\alpha = 0{,}01$), то данная двоичная последовательность не является случайной. В противном случае последовательность носит случайный характер, согласно текущему тесту.

Процесс выполнения статистических тестов в пакете NIST STS выполняется следующим образом [5]:

1) Выбирается последовательность бит S. Её рекомендуемая длина составляет $100 \cdot 10^6$ бит (согласно рекомендации программы NIST STS), однако, так как в настоящем исследовании длины последовательностей формируются из отдельных показаний, полученных с датчиков, а количество было ограничено временем эксперимента, они имеют размер меньше.

2) Для некоторых тестов задаются регулируемые параметры, которые зависят от длины последовательности бит (см. табл. 2) (описание параметров приведено в документации к программе NIST STS).

3) Запускается выполнение статистических тестов. Тестируемая последовательность S делится на m подпоследовательностей S_i ($S = \bigcup_{i=1}^{m} S_i$) длиной 106 бит каждая. Порядок тестирования двоичной последовательности $S_i (i = 1..m)$ для каждого теста состоит из следующих шагов [5]:

а) выдвигается предположение о том, что данная двоичная последовательность S_i случайна;

б) по последовательности S_i вычисляется статистика теста $c(S_i)$;

в) с использованием специальной функции $f(x)$ и статистики теста вычисляется значение вероятности $p\text{-}value = f(c(S_i))$. В качестве $f(x)$ в зависимости от теста используются следующие функции:

$$Q(a,x) \equiv 1 - P(a,x) \equiv$$
$$\equiv \frac{\Gamma(a,x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)} \int_x^{\infty} e^{-t} t^{a-1} dt -$$

неполная гамма-функция,

где $\Gamma(a) = \int_0^{\infty} t^{a-1} t\, dt$ – гамма-функция;

$$erfc = \frac{2}{\sqrt{\pi}} \int_{-x}^{\infty} e^{-u^2} du$$ – дополнительная функция ошибок;

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{-u^2}{2}} du$$ – стандартное нормальное распределение.

г) Если $p\text{-}value \geq 0{,}01$, то последовательность S_i считается случайной.

4) Завершение работы программы. Для каждого теста в отдельности создаётся отчёт, который содержит значения вероятности $p\text{-}value$ и другие параметры, характерные для конкретного теста. Так же все суммар-

Таблица 2

Параметры тестов

Тест	Значение параметра
2. Частотный блочный тест	16384
8. Тест на совпадение неперекрывающихся шаблонов	9
9. Тест на совпадение перекрывающихся шаблонов	9
11. Тест приблизительной энтропии	10
5. Тест на самую длинную последовательность единиц в блоке	18
15. Тест на линейную сложность	500

ные расчетные данные размещаются в файле – отчёте, который отражает результаты всех пройденных тестов.

Последовательность S является случайной, если количество успешных тестов k последовательностей S_i удовлетворяет условию [2], описанному ниже:

$$k \geq \left\lfloor \left(p' - 3\sqrt{\frac{\alpha\, p'}{m}} \right) m \right\rfloor, \qquad (2)$$

где $p' = 1 - \alpha$, $\alpha = 0{,}01$.

4 Результаты тестирования последовательностей

В таблице 3 приведены результаты тестирования последовательностей, сформированных из показаний датчиков. В столбцах указаны датчик, фильтр, применяемый при создании последовательностей, длина последовательностей, наилучшая доля успешно пройденных тестов из 96 последовательностей (равна k/n, где $n = 188$ – общее количество тестов, k – количество успешно пройденных тестов) и количество групп последовательностей, составленных из i-го бита и прошедших все тесты для трёх осей.

В качестве примера на рисунках 4 и 5 приведены результаты тестирования последовательностей (доля успешно пройденных тестов), сформированных из показаний датчика без использования фильтра входных данных и с фильтром 1 соответственно.

Из всех протестированных последовательностей бит, сформированных из показаний датчиков группы «А», не удалось выявить случайные. Применение фильтров увеличивает количество пройденных тестов, однако для выявления случайных последовательностей требуется успешное выполнение всех тестов полностью. Таким образом, можно сделать вывод, что датчики группы «А» не позволяют генерировать случайные последовательности бит предложенными способами.

Таблица 3

Результат тестирования последовательностей

Датчик	Тип фильтра при создании последовательности бит	Длина тестируемой последовательности	Наилучшая доля успешных тестов	Количество групп случайных последовательностей
1A	Без фильтра	$12 \cdot 10^6$	0,82	0
	Фильтр 1	$7 \cdot 10^6$	0,94	0
	Фильтр 2	$11 \cdot 10^6$	0,94	0
2A	Без фильтра	$68 \cdot 10^6$	0,15	0
	Фильтр 1	$6 \cdot 10^6$	0,79	0
	Фильтр 2	$25 \cdot 10^6$	0,13	0
3A	Без фильтра	$25 \cdot 10^6$	0,15	0
	Фильтр 1	$4 \cdot 10^6$	0,95	0
	Фильтр 2	3·106	0,98	0
1B	Без фильтра	$6 \cdot 10^6$	1,00	7
	Фильтр 1	4·106	1,00	10
	Фильтр 2	$8 \cdot 10^6$	1,00	0
2B	Без фильтра	$69 \cdot 10^6$	0,39	0
	Фильтр 1	44·106	0,92	0
	Фильтр 2	$17 \cdot 10^6$	1,00	2
3B	Без фильтра	$30 \cdot 10^6$	0,52	0
	Фильтр 1	$17 \cdot 10^6$	0,95	0
	Фильтр 2	$6 \cdot 10^6$	1,00	3

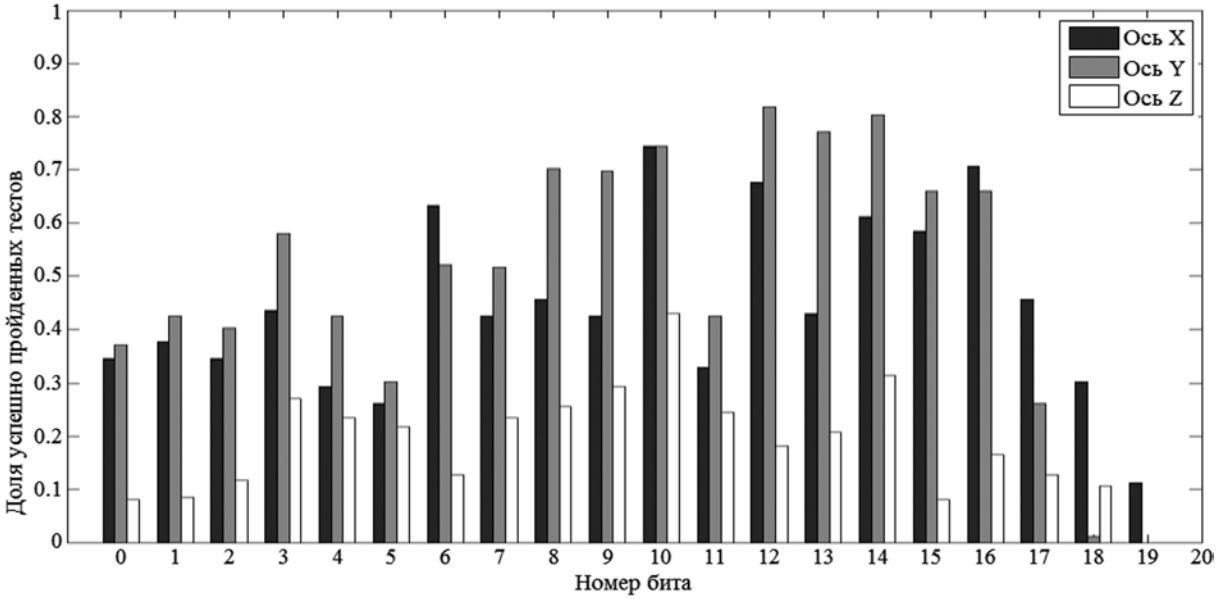

Рис. 4. Результат тестирования датчика 1A без фильтра

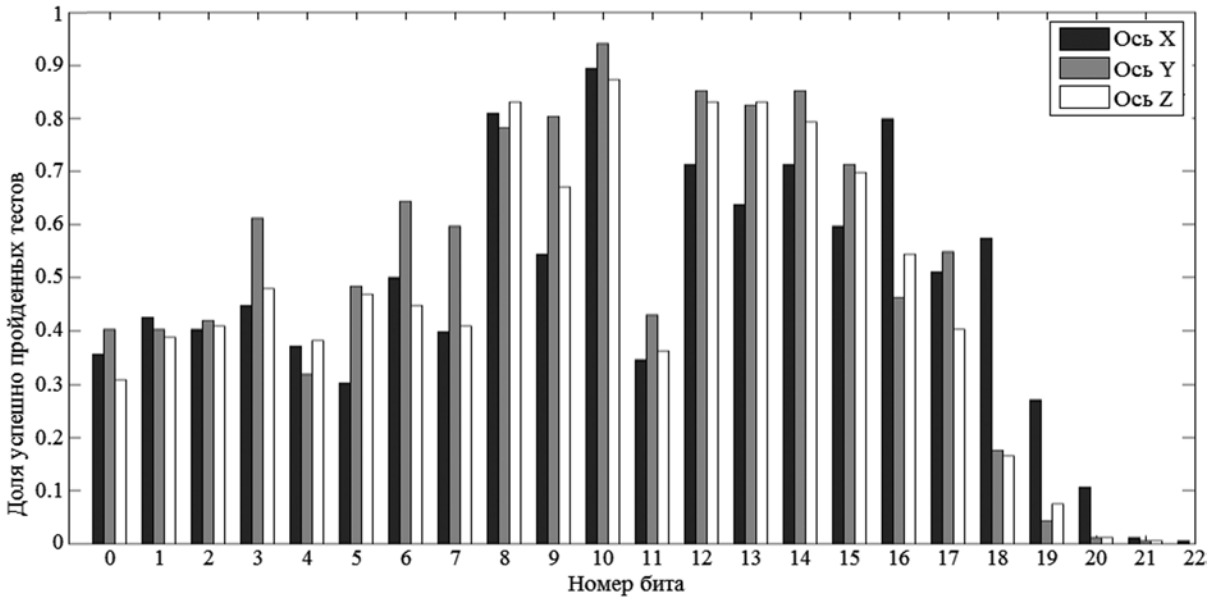

Рис. 5. Результат тестирования датчика 1А с применением фильтра 1

Некоторые последовательности, полученные из показаний датчиков группы «В», прошли все тесты. Для каждого датчика было проведено дополнительное исследование. Для этого формировались новые последовательности путем объединения последовательностей, прошедших все тесты для трёх осей координат. В таблице 4 приведены результаты дополнительных исследований датчиков группы «В». В первом столбце указан датчик, во втором столбце – количество бит одного показания, участвующих в формировании последовательности, скорость датчика (получена экспериментально), максимальная скорость генератора случайных последовательностей на основе показаний датчика (3 оси координат * количество бит * скорость датчика).

Таблица 4

Результат дополнительных исследований

Датчик	Количество бит показания	Скорость датчика (показаний в секунду)	Скорость генератора
1В	9	100	2700
2В	2	200	1200
3В	3	100	900

Заключение

Исследования последовательностей, полученных из показаний датчиков 1В, 2В и 3В, дали положительные результаты. В соответствии с алгоритмом проведения статистического исследования и установленных параметров доверительных интервалов данные последовательности являются случайными.

Скорость генерации последовательности, полученной при помощи датчика 1В, может достигать 2700 бит/с, с использованием датчика 2В – 1200 бит/с и с применением датчика 3В – 900 бит/с. Полученные результаты позволяют генерировать надёжные ключи шифрования за несколько секунд.

Проверка последовательностей бит, сформированных из показаний датчиков 1А, 2А и 3А, выявила статистические отклонения. Поэтому предложенными методами на основе показаний акселерометров мобильных устройств, исследуемых в работе, нельзя генерировать случайные данные.

Исследования показали, что в качестве генератора случайных последовательностей, применяемых в криптографии, можно использовать гироскоп, встроенный в мобильные устройства Digma iDx7, Sony ZR и Samsung Galaxy Note 2.

СПИСОК ЛИТЕРАТУРЫ

1. Фергюсон Н., Шнайер Б. Практическая криптография. – М. : Издательский дом, 2004. – 432 с.

2. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // National Institute of Standards and Technology. – URL: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf (дата обращения: 01.06.2017).

3. Акселерометры и гироскопы. Вибрационные и хроматографические сенсоры // ИНТУИТ. – URL: http://www.intuit.ru/studies/courses/590/446/lecture/9919?page=1 (дата обращения: 01.06.2017).

4. IEEE Standard 754 for Binary Floating-Point Arithmetic // Electrical Engineering and Computer Sciences. – URL: http://www.eecs.berkeley.edu/~wkahan/ieee754status/IEEE754.PDF (дата обращения: 01.06.2017).

5. Потий А., Орлова С., Гриненко Т. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 2. – С. 206–214.

REFERENCES

1. Ferguson N., Schneier B. *Prakticheskaia kriptografiia* [Practical Cryptography]. Moscow, Izdatelskii dom Publ., 2004. 432 p.

2. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *National Institute of Standards and Technology.* Available at: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf (accessed: 01.06.2017).

3. Akselerometry i giroskopy. Vibratsionnye i khromatograficheskie sensory [Accelerometers and Gyroscopes. Vibration and Chromatography Detectors]. *Intuit.* Available at: http://www.intuit.ru/studies/courses/590/446/lecture/9919?page=1 (accessed: 01.06.2017).

4. IEEE Standard 754 for Binary Floating-Point Arithmetic. *Electrical Engineering and Computer Sciences.* Available at: http://www.eecs.berkeley.edu/~wkahan/ieee754status/IEEE754.PDF (accessed: 01.06.2017).

5. Potii A., Orlova S., Grinenko T. Stastisticheskoe testirovanie generatorov sluchainykh i psevdosluchainykh chisel s ispolzovaniem nabora statisticheskikh testov NIST STS [Statistical Testing of Random and Pseudorandom Number Generators by the Use of NIST STS Statistical Tests]. *Pravove, normativne ta metrologichne zabezpechennia sistemi zakhistu informatsii v Ukraini* [Legal, Regulatory and Metrological Support Information. Scientific and Technical Journal], 2001, no 2, pp. 206–214.