ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ЧЕЛОВЕКО- МАШИННОГО ВЗАИМОДЕЙСТВИЯ

Статья посвящена разработке и анализу программного генератора случайных чисел основанного на человеко-машинном взаимодействии для программных и криптографических приложений. Описан метод генерации случайных чисел основанный на человеко-машинном взаимодействии, с использованием времени и положения курсора на дисплее компьютера или смартфона. На основе этого метода разработан и программно реализован генератор случайных чисел. Проведен предварительный анализ алгоритма, в ходе которого было сгенерировано 11000 чисел. Создано тестовое программное обеспечение для данного метода, рассмотрены предварительные показатели генерируемых случайных чисел. Показано, что функция распределения случайных чисел имеет равномерный вид. Преимуществом рассматриваемого генератора является простота в изготовлении и эксплуатации.

Ключевые слова: человеко-машинное взаимодействие, генератор, случайные числа, криптография, статистическое тестирование.

Averin A. S., Zyulyarkina N. D., Izhberdeeva E. M.

RANDOM NUMBER GENERATOR BASED ON HUMAN-COMPUTER INTERACTION

The paper is devoted to the development and analysis of a software random number generator based on human-computer interaction for software and cryptographic applications. Described is a method of generating random numbers based on human-computer interaction, using time and position of a cursor on a computer or smartphone display. Based on this method, a random number generator has been developed and programmatically implemented. A preliminary analysis of the algorithm was performed, during which 11,000 numbers were generated. The test software for this method has been created, preliminary indicators of generated random numbers have been considered. The random number distribution function is shown to be uniform. The advantage of this generator is its ease of manufacture and operation.

Keywords: *human-computer interaction, generator, random numbers, cryptography, statistical testing.*

Введение. В настоящее время крайне актуальной является проблема генерации случайных чисел с дальнейшей целью применения их в системах защиты информации. Характеристики систем безопасности в большинстве своем зависят от характеристик их криптографических подсистем, которые определяются, как правило, показателями используемых генераторов случайных чисел, так как на их базе создаются ключи шифрования и защитные последовательности [1]. Так же, можно отметить важную роль генераторов случайных чисел в таких областях знаний как, численный анализ, теория игр, теория принятия решений и моделирование.

Для генерации таких чисел используется несколько подходов. Первый из них связан с созданием и применением специальных устройств, использующих какие-либо физические источники шума. Второй подход связан с получением случайных величин на обычном персональном компьютере без применения дополнительного оборудования. Учитывая это, актуальным может стать способ, связанный с использованием стандартных устройств компьютера. Наиболее распространенным методом генерации случайных чисел, использующим этот подход, является генерация случайных чисел с использованием счетчика тактов процессора. К его недостаткам можно отнести чувствительность фазового шума генераторов частоты к внешним помехам, а значит, возможность влиять на генератор случайных чисел извне [2]. Так же генераторы случайных чисел могут строиться на фундаментальных законах физики, функциональных или «паразитных» свойствах электронных приборов и компьютерных систем, свойствах элементов электронных схем [3].

Целью данной работы является описание алгоритма генерации случайных чисел основанного на человеко-машинном взаимодействии, с использованием времени и положения курсора на дисплее компьютера или смартфона. Генератор случайных чисел, представленный в этой работе, разрабатывался как часть алгоритма консенсуса для блокчейн систем.

Существующие решения. В настоящее время существует большое количество пред-

лагаемых решений в области генерации случайных чисел. Рассмотрим некоторые из них:

1. Аппаратный генератор случайных чисел, представленный в статье [1] Р.О. Султановым и Д.В. Лопатиным. Для связи с ПК в описанном генераторе авторами используется микроконтроллер с оригинальным программным обеспечением. Для работы с шиной USB использовалась открытая библиотека пользовательских функций, создано программное обеспечение для типовых задач, рассмотрены качественные показатели генерируемых случайных чисел. Показано, что функция распределения случайных чисел имеет равномерный вид. В преимуществах аппаратного генератора случайных чисел отмечается то, что он обладает простотой в изготовлении (тиражировании) и эксплуатации [1].

2. Генератор случайных чисел на базе звуковой карты, представленный в статье [4] Д.Б. Беспаловым и С.В. Белим. В качестве источника внешней энтропии рассматривается линейный вход звуковой карты. Этот разъем предназначен для подключения источников аналогового звукового сигнала, принимаемого на входе звуковой карты. Сигнал переводится в последовательность байтов с помощью аналого-цифрового преобразователя, к действию полезного сигнала постоянно добавляется шум, вызванный электромагнитными наводками от других элементов цепи, тепловым шумом в цепях питания и прочими флуктуациями в подсистеме аналогового входа [4]. Для считывания данных с линейного входа звуковой карты авторами была написана программа. Программа позволяет составить список устройств. Преимуществом называется цена «создания» работающего устройства, пользователь платит за программное обеспечение, а аппаратной составляющей не требуется.

3. Генератор случайных чисел с неравномерным распределением с помощью веб-камеры компьютера представленный в статье «Генератор Случайных Чисел С Неравномерным Распределением» [5] Р.М. Михерского, М.В. Исаева и Д.М. Полянчука. Для генерации случайных чисел с неравномерным распределением необходимо, чтобы веб-камера, подключенная к ноутбуку или компьютеру,

находилась в темном помещении или была закрыта [5]. Размер каждого снимка – 640 на 480 пикселей, из каждой фотографии извлекается матрица пикселей. Далее для 24-х разрядного изображения каждый пиксель содержит в себе информацию о трех цветах (для цветовой модели RGB) – соответственно красном, зеленом и синем. На каждый цвет отводится 8 бит, то есть максимально возможное значение в десятичном представлении – 255, а минимальное 0. Значению 255 соответствует максимальная интенсивность цвета, а значению 0 – минимальная. На следующем шаге, в общем случае формируется двумерный массив, в который записываются соответствующие значения разностей компонент цвета двух изображений для каждого из пикселей. Полученные разности могут изменяться от – 255 до 255. Эти разности и являются случайными числами [5].

4. Особо интересным примером реализации является генератор случайных чисел от компании «Код безопасности», разработчик криптографического комплекса «Континент», получила патент на биологический датчик случайных чисел. С описанием патента, возможно, ознакомиться на сайте Роспатента и доступно по ссылке: http://www1.fips.ru/fips_servl/fips_servlet?DB=RUPAT&DocNumber=2628213&TypeFile=html). В основе случайности лежит реакция пользователя на показанное ему изображение. «Компания уверяет, что до нее такие технологии в мире не патентовались». Датчик генерирует случайные последовательности, основываясь на скорости и точности реагирования руки пользователя на изменение изображения на экране ПК или планшета, для ввода используются мышь или тачскрин. В случайные моменты времени, определяемые кликами пользователя, измеряются меняющиеся во времени значения определенного набора величин, связанных с псевдослучайным процессом. Затем полученные случайные значения величин процесса отображаются в последовательность бит, к которой применяется функция хеширования. Так же компания на своем официальном сайте <https://www.securitycode.ru/> пишет о том что: «Известные исследования подтверждают, что движения мышью или нажатия клавиш порождают предсказуемые последовательности чисел, которые нельзя напрямую использовать в задачах криптографии. Таким образом, общеизвестные способы требуют модификации и доработки» [7].

Предлагаемый алгоритм генерации случайных чисел на основе человеко-машинного взаимодействия. Был проведен анализ того, как часто люди взаимодействуют с компьютерами и смартфонами, на январь 2020 года. Согласно отчету о состоянии цифровой сферы Digital 2020, который каждый год готовят We Are Social и Hootsuite количество интернет-пользователей в мире составляет 4,54 миллиарда и более 5,19 миллиарда человек пользуются мобильными телефонами. Так же стоит заметить, что среднестатистический человек проводит онлайн 6 ч 40 мин в сутки, в то время как в 2018 году проводил только 6 ч, а суммарно люди проведут онлайн за 2020 год один миллиард двести пятьдесят тысяч лет. Это говорит о том, что способ использования такого ресурса, как человеко-машинное взаимодействие может быть крайне эффективен. Важным преимуществом разрабатываемого алгоритма генерации случайных чисел является его независимость от дополнительных устройств, достаточно встроенных в любой смартфон дисплея и манипулятора.

В ходе разработки алгоритма консенсуса для блокчейн систем был создан алгоритм генерации случайных чисел на основе человеко-машинного взаимодействия. Данный алгоритм использует в своей работе функцию от времени и координат курсора в реальном времени (см. рис. 1).

Результатом является вектор из 24 случайных величин, из которых нами рассматриваются 19 (с 3 по 21). Это объясняется тем, что визуальный анализ показывает несоответствие рассматриваемому критерию - равной вероятности появления для всех цифр на каждой позиции. Процесс генерации случайных чисел происходит в момент взаимодействия пользователя с компьютером, планшетом или смартфоном. При этом процесс генерации случайных чисел проходит в фоновом режиме, то есть, остается незаметным для пользователя. В сравнении с генератором случайных чисел от компании «Код безопасности», предложенному алгоритму не требуется входных данных.

Предварительно функция от времени и координат курсора в реальном времени использует результаты делений реального времени на каждую координату дисплея поддельности, и сумму полученных результатов. Используется непрерывное течение времени в микросекундах и положение курсора, полу-

Рис. 1. Процесс получения случайных чисел

Таблица 1

Статистика значений случайных величин

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	1219	1127	1113	1125	1139	1089	1096	1093	1122	1146	1090	1119	1053	1120	1097	1146	1083	1120	1051	1113	1164	1312	2145
1	2513	1192	1079	1129	1124	1108	1130	1103	1104	1123	1069	1081	1121	1059	1139	1056	1086	1155	1088	1118	1072	1085	909	0
2	1764	1140	1080	1068	1061	1076	1138	1127	1110	1090	1121	1104	1133	1109	1067	1122	1111	1126	1096	1084	1106	1154	1227	2236
3	1375	1140	1063	1148	1095	1111	1081	1101	1102	1128	1088	1082	1118	1131	1076	1107	1166	1114	1068	1070	1077	1044	843	0
4	1173	1152	1068	1036	1111	1087	1134	1041	1086	1063	1117	1112	1013	1150	1091	1094	1155	1006	1117	1088	1112	1149	1324	2131
5	1021	1061	1154	1112	1179	1096	1035	1058	1144	1089	1102	1124	1145	1044	1100	1131	1088	1082	1134	1138	1122	1060	905	0
6	920	1036	1104	1071	1076	1097	1040	1143	1134	1101	1123	1040	1115	1086	1049	1118	1052	1102	1155	1103	1127	1164	1359	2229
7	824	1041	1048	1137	1084	1043	1140	1082	1135	1150	1051	1124	1122	1104	1143	1088	1060	1108	1071	1141	1063	1045	875	0
8	720	1094	1144	1123	1056	1133	1100	1116	1013	1088	1108	1126	1044	1156	1111	1079	1068	1093	1070	1097	1105	1077	1314	2260
9	691	926	1134	1064	1090	1111	1114	1134	1080	1047	1076	1118	1071	1109	1105	1109	1069	1132	1082	1111	1104	1059	933	0
$\chi^2_{набл}$	3776,9	61,8	11,54	11,47	10,89	6,30	12,37	8,71	11,50	8,04	6,84	6,09	14,99	12,72	7,51	4,06	14,40	13,17	7,38	6,63	3,90	21,55	402,9	11013,3

Таблица 2

Критические области для хи-квадрат распределения

n - 1	.995	.990	.975	.950	.900	.750	.500	.250	.100	.050	.025
9	1.73493	2.08790	2.70039	3.32511	4.16816	5.89883	8.34283	11.38875	14.68366	16.91898	19.02277

ченные данные подставляются в функцию, полученную экспериментальным. Процесс получения случайных чисел представлен на рис. 1. В ходе предварительного анализа, была собрана тестовая выборка из 11000 сгенерированных чисел. Данная выборка собиралась на экране с разрешением 1366 на 768 px. Далее в табл. 1, представлена статистика того какие значения и как часто принимались случайными величинами.

Из табл. 1 следует, что крайние значения в выборке, очевидно, не удовлетворяют искомым требованиям, поэтому в дальнейшем мы исключаем их анализа. Далее на рис. 2 показана статистика из табл. 1 в виде графиков распределения для каждой рассматриваемой случайной величины:

Следует отметить, что на графиках демонстрируется частота появления значений, в

результате генерации, для всех случайных величин на каждой позиции (с 3 по 21) близка к равномерному. На графиках черная линия соответствует 1100.

Была проведена проверка гипотезы о равномерном распределении при помощи критерия согласия Пирсона. Ее результаты представлены в нижней части на табл. 1, а также на табл. 2. (Критические области для хи-квадрат распределения) можно сравнить соотвествие уровню значимости полученных результатов.

Согласно результатам, для вертикальных выборок от 3 до 21 можно сказать, что: при уровне значимости $\alpha = 0,05$ выборочные данные не противоречат тому, что данные случайные величины имеют дискретное равномерное распределение.

Из анализа представленных данных мож-

Рис. 2. Графики распределения случайных величин

но сделать вывод, что дальнейшее исследование и анализ генератора случайных чисел, основанного на человеко-машинном взаимодействии, является целесообразным.

Заключение. В результате данной работы был описан алгоритм генерации случайных чи-

сел на основе человеко-машинного взаимодействия, с использованием времени и положения курсора на дисплее компьютера или смартфона.

Было рассмотрено несколько ранее опубликованных решений в сфере генерации случайных чисел. В том числе решение, пред-

ставленное компанией «Код безопасности». В сравнении с данными решениями алгоритм генерации случайных чисел на основе человеко-машинном взаимодействии имеет ряд преимуществ:

- не требуется дополнительное оборудование, будь то: микроконтроллер, аудио разъем или веб-камера;
- отсутствует необходимость использования, каких-либо изображений для работы генератора;
- генератор способен работать в фоновом режиме, абсолютно не заметно для пользователя.

Проведен предварительный анализ алгоритма, в ходе которого было сгенерировано 11000 чисел. Создано тестовое программное обеспечение для представленного метода,

рассмотрены предварительные показатели генерируемых случайных чисел. Получено, что выборочные данные соответствуют тому, что распределение случайных величин является дискретным равномерным.

Безусловно, в дальнейшем необходимо увеличить количество итераций и провести исследование полученных материалов на критерий соответствия требованиям, предъявляемых к генераторам случайных чисел. Дальнейшее исследование и анализ генератора случайных чисел, основанного на человеко-машинном взаимодействии, является целесообразным и может быть продолжено в дальнейшем.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Султанов Р. О., Лопатин Д. В. Аппаратный генератор случайных чисел // Гаудеамус. 2013. №2 (22). URL: <https://cyberleninka.ru/article/n/apparatnyy-generator-sluchaynyh-chisel> (дата обращения: 25.04.2020).
2. Реализация генераторов случайных чисел / А. В. Ковалев // Научная сессия МИФИ. 2007. Том 12. С. 176–177.
3. Григорьев А. Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей // Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, С. 22–28.
4. Беспалов Д. Б., Белим С. В. Реализация генератора случайных чисел на базе звуковой карты // МСиМ. 2010. №1 (21). URL: <https://cyberleninka.ru/article/n/realizatsiya-generatora-sluchaynyh-chisel-na-baze-zvukovoy-karty> (дата обращения: 25.04.2020).
5. Михерский Р.М., Исаев М.В., Полянчук Д.М. ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ С НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ // Вестник Физико-технического института Крымского федерального университета имени В. И. Вернадского. 2018. №1. URL: <https://cyberleninka.ru/article/n/generator-sluchaynyh-chisel-s-neravnomernym-raspredeleniem> (дата обращения: 25.04.2020).

References

1. Sultanov R. O., Lopatin D. V. Apparatty generator sluchaynykh chisel // Gaudeamus. 2013. №2 (22). URL: <https://cyberleninka.ru/article/n/apparatnyy-generator-sluchaynyh-chisel> (data obrashcheniya: 25.04.2020).
2. Realizatsiya generatorov sluchaynykh chisel / A. V. Kovalev // Nauchnaya sessiya MIFI. 2007. Tom 12. C. 176–177.
3. Grigor'yev A. YU. Metody testirovaniya generatorov sluchaynykh i psevdosluchaynykh posledovatel'nostey // Uchenyye zapiski UIGU. Ser. Matematika i informatsionnyye tekhnologii. UIGU. Elektron. zhurn. 2017, № 1, S. 22–28.
4. Bespalov D. B., Belim S. V. Realizatsiya generatora sluchaynykh chisel na baze zvukovoy karty // MSiM. 2010. №1 (21). URL: <https://cyberleninka.ru/article/n/realizatsiya-generatora-sluchaynyh-chisel-na-baze-zvukovoy-karty> (data obrashcheniya: 25.04.2020).
5. Mikherskiy R.M., Isayev M.V., Polyanchuk D.M. GENERATOR SLUCHAYNYKH CHISEL S NERAVNOMERNYM RASPREDELENIEM // Vestnik Fiziko-tekhnicheskogo instituta Krymskogo federal'nogo universiteta imeni V. I. Vernadskogo. 2018. №1. URL: <https://cyberleninka.ru/article/n/generator-sluchaynyh-chisel-s-neravnomernym-raspredeleniem> (data obrashcheniya: 25.04.2020).

АВЕРИН Андрей Сергеевич, аспирант кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). Россия, 45408, г. Челябинск, пр. Ленина, 76. E-mail: andreaverin24@gmail.com.

ЗЮЛЯРКИНА Наталья Дмитриевна, доктор физико-математических наук, доцент, профессор кафедры «Защита информации» ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). Россия, 454080, г. Челябинск, пр. Ленина, 76. E-mail: ziuliarkinand@susu.ru.

ИЖБЕРДЕЕВА Елизавета Монировна, студент кафедры теории управления и оптимизации ФГБОУ ВО «Челябинский государственный университет». Россия, 454001, г. Челябинск, ул. Братьев Кашириных, 129. E-mail: elizaveta.izhberdeeva@gmail.com.

AVERIN Andrey, Postgraduate Student, Department of Information Security, South Ural State University (National Research University). 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: andreaverin24@gmail.com.

ZYULYARKINA Natalya, Doctor of Physics and Mathematics, Associate Professor, Professor of the Department of Information Security, "South Ural State University (national research university)". 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ziuliarkinand@susu.ru.

IZHBERDEEVA Elizaveta, student of the Department of Control Theory and Optimization, "Chelyabinsk State University". Russia, 454001, Chelyabinsk, Kashirin Brothers Street, 129. E-mail: elizaveta.izhberdeeva@gmail.com.