Оценка качества генератора случайных чисел с помощью тестов DIEHARD

В настоящее время генераторы случайных чисел (ГСЧ) широко применяются в самых разных областях человеческой жизнедеятельности. Их используют, например, в криптографии и информационной безопасности, научных и социологических исследованиях, играх и лотереях – в общем, в тех сферах, где необходимо иметь дело с числами или событиями, выбранными случайно, то есть независимо друг от друга, без прослеживаемых закономерностей.

Соответственно, качество ожидаемого результата будет зависеть от качества используемого ГСЧ, насколько сгенерированные им числа, а также последовательности таких чисел случайны и независимы друг от друга.

Таким образом, возникает проблема оценки качества ГСЧ, для понимания возможности и целесообразности использования того или иного ГСЧ для решения поставленных задач.

В орган по сертификации Системы добровольной сертификации программного обеспечения и аппаратно-программных комплексов (СДС ПО и АПК) было представлено на тестирование программное обеспечение (ПО), содержащее генератор случайных чисел (ГСЧ) и используемое при проведении лотерей.

ПО содержит в своем составе генератор псевдослучайных чисел (ГПСЧ) – разновидность ГСЧ, который генерирует случайные числа по заданному алгоритму, используя в качестве источника энтропии шум звуковой карты, встроенной в материнскую плату компьютера, на котором устанавливается данное ПО.

Перед экспертами органа по сертификации была поставлена задача оценить качество ГПСЧ. Основными критериями оценки качества ГПСЧ являются соответствие генерируемых последовательностей равномерному распределению и отсутствие в последовательностях детерминированных закономерностей.

Для оценки качества представленного ГПСЧ был выбран набор тестов DIEHARD [1] как один из наиболее авторитетных в области тестирования ГСЧ.

Данный набор тестов носит полное наименование DIEHARD: A BATTERY OF TESTS OF RANDOMNESS (на русский язык можно перевести как «Набор статистических тестов Крепкий орешек») и был разработан американским математиком Дж. Марсалья (George Marsaglia, 1924-2011), профессором университетов штатов Вашингтон и Флорида, посвятившим свою жизнь исследованию случайных чисел.

Набор состоит из 18 тестов, большинство которых является уникальной разработкой автора, их описание на русском языке можно найти в [2] или [3]. Сам автор заявляет о 15 тестах, но один из тестов («Count the 1’s» – «Подсчет единиц) разбит на два, а другой («OPSO, OQSO and DNA») содержит в себе три теста.

Для тестирования ГСЧ тестами DIEHARD необходим массив случайных чисел, сгенерированный исследуемым ГСЧ, и содержащий минимум 80 млн. бит, преобразованных в 32-битные числа.

Результатами тестов являются вычисленные значения *p-value* в количестве 220 шт., которые должны быть равномерно распределены в диапазоне [0, 1], если исходный массив случайных чисел содержит истинно независимые случайные биты. *P-value* представляет собой вероятность ошибки при отклонении нулевой гипотезы и является значением функции *F(x)*, где *F* – предполагаемое распределение эталонной случайной переменной *x*. Нулевой гипотезой H_0 в математической статистике называется утверждение, которое необходимо опровергнуть, проведя исследование статистических данных. Отвергая нулевую гипотезу H_0, принимают альтернативную гипотезу H_a, которая должна быть противоположна нулевой гипотезе. При этом задают уровень значимости α, который является вероятностью отклонить гипотезу H_0 когда она на самом деле верна (т.н. «ошибка первого рода»). Популярные уровни значимости α – 0,1; 0,05; 0,01. В нашем случае нулевой гипотезой будет утверждение, что испытываемый ГПСЧ производит независимые случайные числа. В качестве альтернативной гипотезы будет выступать утверждение, что случайные числа, производимые данным ГПСЧ, не являются независимыми и случайными. Уровень значимости α в нашем случае был выбран равным 0,05.

В наборе тестов DIEHARD имеется работоспособная DOS-реализация этих тестов, которая свободно запускается в операционных системах семейства Windows (была успешно опробована на Windows XP, 7 и 10). В качестве выходных данных выдается текстовый файл, содержащий краткое описание тестов и вычисленные значения *p-value*.

Сам автор предлагает следующую интерпретацию своих тестов: «Большинство тестов DIEHARD выдают величины *p-value*, которые должны быть равномерно распределены на интервале [0,1], если входной файл содержит действительно независимые случайные биты. Эти *p-value* являются корнями функции *F(x)*, где *F* – предполагаемое распределение выборочной случайной величины *x* – часто нормальное. Но это предполагает, что *F* является асимптотической аппроксимацией, для которой соответствие будет наихудшим на хвостах функции. Таким образом, не стоит удивляться случайным значениям *p-value* около 0 или 1, например 0,0012 или 0,9983. Когда массив данных действительно проваливает тесты, вы получите *p-value*, равные 0 или 1, в шести или более местах среди результатов тестов. Не стоит думать, что 0,975 < *p-value* < 0,025 означает, будто ГСЧ не прошел тест при уровне значимости 0,05. Такие значения случаются среди сотен, которые производит DIEHARD, даже с качественными ГСЧ».

С помощью исследуемого ПО было сгенерировано десять файлов случайных чисел объемом 96 млн. бит каждый. Результаты обработки этих десяти файлов тестами DIEHARD – 2200 значений *p-value* – представлены в таблице 1.

Как видно, в результатах нет ни одного значения *p-value* строго равного нулю или единице. Несмотря на предупреждение автора о т.н. «хвостах» функции *F(x)*, жирным выделены значения 0,975 < *p-value* < 0,025, теоретически отвергающие нулевую гипотезу при уровне значимости α = 0,05.

Таблица 1

N	Название теста	P-value
1	Birthday Spacings (Дни рождения)	0,675140 0,744750 0,256665 0,271650 0,498370 0,094682 0,298645 0,668362 0,619930 0,360606 0,358579 0,220879 0,549370 **0,017710** 0,064065 0,645644 0,208634 0,202022 **0,991689** 0,827728 0,341058 0,456683 **0,008315** 0,241258 0,183753 0,499637 0,387891 0,557767 0,606439 0,832215 0,697638 0,839240 **0,007578** 0,855052 0,625418 0,810140 0,947914 0,357638 0,268187 0,642928 0,689977 0,480138 0,667789 0,329183 0,076252 0,750567 0,421622 0,676916 0,190355 0,263963 0,217529 0,388760 0,028198 0,441918 **0,008894** 0,576710 0,175686 0,936139 0,609240 0,747696 0,058597 0,114042 0,489795 0,757435 0,093591 0,221495 0,734980 0,623944 0,867229 0,330272 0,047480 0,678792 0,818501 **0,980954** 0,545057 0,534595 0,030932 0,906659 0,800710 0,711356 0,413099 0,055977 0,522383 0,210756 0,613113 0,891610 0,638174 0,241745 0,598375 0,132461 0,866126 0,032227 0,262340 0,448553 0,092145 0,181019 0,802538 0,675063 0,919717 0,120920
2	Overlapping Permutations (Пересекающиеся перестановки)	0,618784 0,619420 0,323374 0,755202 0,635486 0,052678 0,051742 0,103244 0,055530 0,209458 **0,999995** **0,985567** 0,581157 0,131261 0,334859 **0,000956** 0,253619 **0,999716** 0,239769 0,478627
3	Ranks of Matrices 31x31 (Ранги матриц 31x31)	0,674671 0,889697 0,713599 0,447385 0,321398 0,384058 0,368872 0,579963 0,430027 0,627832
4	Ranks of Matrices 32x32 (Ранги матриц 32x32)	0,336459 0,336419 0,418641 0,475730 0,364586 0,340065 0,332283 0,507574 0,330238 0,833796
5	Ranks of Matrices 6x8 (Ранги матриц 6x8)	0,69245 0,86721 0,22261 0,61713 0,52050 0,55486 **0,02214** 0,13625 0,23098 0,62397 0,51060 0,88715 0,50413 0,50731 0,20699 0,22402 0,61327 0,10669 0,49187 0,66307 0,58678 0,79747 0,73875 0,95674 0,03231 0,269997 0,427858 0,089160 0,899849 0,962987 0,431871 0,949488 0,463781 0,047842 0,033558 0,397365 0,373894 0,230533 0,290698 0,763063 0,351815 0,496317 0,957421 0,782010 0,947578 0,129911 0,387241 0,049254 0,827402 0,479822 0,226667 0,476302 0,802662 0,317820 0,835749 0,123267 0,141133 0,591262 0,237731 0,040351 0,217951 0,856148 0,779866 0,919976 **0,978686** 0,069619 0,236149 0,576366 0,393905 0,356133 0,214863 0,035774 0,686624 0,121020 0,556534 0,797965 0,716951 0,285694 0,84148 0,96602 0,41496 0,96228 0,952146 0,791494 0,438007 0,216050 0,168223 0,270849 0,082121 0,972110 0,849949 0,552981 0,188069 0,773728 0,903716 0,114664 0,859536 0,864328 0,642387 **0,007984** 0,038322 0,064039 0,295019 0,816616 0,217068 0,688215 0,421788 0,673298 0,316864 0,845914 0,406018 0,055055 0,944589 0,516776 0,329952 0,593764 0,241992 0,368567 0,849247 0,494588 0,272326 0,355706 0,609704 0,915765 0,053877 0,499795 0,256396 **0,002875** 0,499008 0,476527 0,532542 0,074343 0,281324 **0,004988** 0,382025 0,496163 0,110353 0,372356 0,758417 0,238241 0,438946 0,216565 0,152550 0,157100 0,872186 0,460553 0,263367 0,865073 0,368393 0,662613 0,626902 0,708782 0,425796 0,218978 0,246994 0,902133 0,549216 0,723096 0,459320 **0,015160** 0,025558 0,203513 **0,002837** 0,132579 0,185839 0,755456 0,917144 0,032529 0,157009 0,657355 0,313493 0,028132 0,892675 0,715730 0,863575 0,097967 0,937512 0,544495 0,388217 0,033412 0,840968 0,959830 0,593770 0,327696 0,548906 0,104841 0,535613 0,747758 0,761547 0,241538 0,265986 0,391947 0,378840 0,173660 0,381869 0,745399 0,363805 0,331973 0,295533 0,514240 0,435959 0,888459 0,191915 0,158662 0,649324 **0,006010** 0,201898 0,896060 0,087751 0,305055 0,673678 0,617471 0,368977 0,940825 0,890441 0,681203 0,838866 0,084754 0,262632 0,088759 0,173210 0,935403 0,151008 0,035432 0,400063 0,607107 0,839028 0,958745 0,950793 **0,000170** 0,108205 0,318366 0,450305 0,669334 0,025979 0,038064 0,486356 0,235187 0,413342 0,212850 0,513351 0,370867 0,067464 0,510906 0,749543 0,383473 0,331766 0,344347 0,450516 0,309034 0,800574 0,409513 0,255126 0,873918 0,777285 0,970025 0,287630 0,728679 **0,008043** 0,783852
6	Bitstream (Поток битов)	0,76818 0,23277 0,67874 0,33932 0,95040 0,64545 0,53878 0,46990 **0,02030** 0,81374 0,76172 0,03173 **0,00754** 0,53135 0,76890 0,70826 0,34619 0,61280 0,56282 0,72017 0,15847 0,84564 0,62615 0,33420 0,93095 0,27462 0,20058 0,60832 0,90993 0,36096 0,59116 0,86680 0,39829 0,72953 **0,02322** 0,20255 0,15455 0,54712 0,77734 0,66012 0,28405 0,83889 0,85963 0,41460 0,24143 0,92045 0,05623 0,32827 0,11840 0,59207 0,66948 0,40280 0,69529 0,83076 0,32406 0,80484 0,54156 0,47734 0,59116 0,83717 0,19993 0,46711 0,82420 0,43106 0,35224 0,02870 0,80095 0,80225 0,95159 0,30499 0,32322 0,31405 0,49690 0,46711 0,57292 0,15234 0,25624 0,38483 0,29766 0,13287 0,94771 0,20189 0,30663 0,80290 0,37859 0,81122 0,37859 0,95654 0,64892 0,28802 0,59298 0,18460 0,06521 0,35224 0,46618 0,83252 0,13540 0,04897 0,66948 0,79437 0,48665 0,24509 0,55729 0,57658 0,13187 **0,01034** 0,09406 0,81059 0,79303 0,72875 0,48758 0,82420 0,57384 0,92649 0,72409 0,95802 0,91586 0,88944 0,59570 0,62526 0,07829 0,76676 0,89378 0,15124 0,07232 0,40280 0,53878 0,23636 0,29122 0,22290 0,19602 0,89464 0,52764 0,52391 0,12743 0,32071 0,67707 0,53321 0,09683 0,47734 0,63496 0,73415 0,02676 0,47641 0,26230 0,61637 0,31074 0,82600 0,42373 0,57475 0,21258 **0,97844** 0,32490 0,46711 **0,00528** 0,95523 0,13237 0,77032 0,02870 **0,01614**

N	Название теста	P-value									
		0,71622	0,30581	0,66524	0,77173	0,13337	0,05784	**0,98490**	0,29042	0,97285	0,31488
		0,95781	0,91182	0,92045	0,06823	0,22220	0,86478	0,56282	0,74552	0,65152	0,96224
		0,49410	0,31904	0,56097	0,58298	0,51460	0,54805	**0,97525**	0,61190	0,25474	0,61904
		0,51181	0,90917	0,78765	0,10723	0,59751	0,28010	0,70019	0,09250	0,72487	0,84172
7	Overlapping Pairs Sparse Occupancy (Проверка разреженных пересекающихся пар)	0,9506	0,4556	0,2580	0,4652	0,2007	0,1847	0,1847	0,8874	0,1738	0,7184
		0,7090	0,8641	0,6525	0,9703	0,6995	**0,9779**	0,1431	0,7756	0,5909	0,6029
		0,6358	0,8880	0,3712	0,6280	0,4243	0,9127	0,1783	0,8840	0,6227	0,5707
		0,4858	0,8671	0,8166	0,3167	0,2890	0,3557	0,3033	0,2481	0,4488	0,0570
		0,7566	0,2046	0,6056	0,0685	0,6947	0,0746	0,6280	0,7412	0,2525	0,2961
		0,3069	0,5949	0,3069	0,4721	0,3253	0,0535	0,7196	**0,9870**	0,3856	0,3094
		0,1045	0,5298	0,4461	0,1502	0,2320	0,4082	0,7725	0,1774	0,7725	0,6148
		0,4379	0,9691	0,1559	0,8054	0,3021	0,8247	0,0925	0,3493	0,7007	0,5421
		0,4243	0,8119	0,6911	0,4230	0,9094	0,0931	0,8166	0,9299	0,8663	0,3118
		0,8166	0,1838	**0,9785**	0,8685	0,1189	**0,0012**	0,6280	0,2682	0,6525	0,0547
		0,4707	0,6240	0,1210	0,2636	0,5106	0,9374	0,2961	0,4502	0,2289	0,9569
		0,9395	0,5721	0,8994	0,0653	0,1392	0,2603	0,1462	**0,0077**	0,1196	0,1703
		0,0296	0,6109	0,2614	0,7356	0,4447	0,3429	0,2514	**0,9965**	0,8926	0,4082
		0,3429	0,7288	0,4748	0,8501	0,8419	0,6911	0,0454	0,2247	0,3634	**0,9969**
		0,4461	0,7367	0,1695	0,3856	0,4625	0,8611	0,5462	0,5694	0,3033	0,9451
		0,4679	0,1494	0,5366	0,4203	0,6306	0,9742	0,8044	0,9226	0,2125	0,6800
		0,4872	**0,9992**	0,2973	0,6886	0,6886	0,1703	**0,0183**	0,1033	0,0578	0,7322
		0,7534	0,0811	0,5092	0,4257	0,4830	0,5734	0,1238	0,2831	0,6651	0,0886
		0,1149	0,1462	0,7423	0,5748	0,8193	**0,9910**	0,8308	0,9679	0,8256	0,2299
		0,1783	0,2773	0,0528	0,7288	0,0375	**0,0174**	0,6800	0,5188	0,9339	0,2762
		0,9523	0,1559	0,5571	0,1189	0,3493	0,1601	0,5161	0,1893	0,5051	0,6188
		0,4995	0,8101	0,8900	0,8015	0,4666	0,9361	0,5503	0,8334	0,9666	0,5815
		0,9933	0,3241	0,1423	0,4379	0,7412	0,0770	0,1089	0,2614	0,0937	0,4940
8	Overlapping Quadruples Sparse Occupancy (Проверка разреженных пересекающихся четверок)	0,5104	**0,9798**	0,6600	0,1511	0,5841	0,2286	0,6952	0,4901	0,7779	0,8652
		0,8531	0,8752	0,0277	0,2946	0,5036	0,1418	0,3135	0,9021	0,6612	0,2946
		0,8585	0,2796	0,4416	0,3208	0,0901	0,3992	0,8206	0,5360	0,8912	0,8258
		0,4163	0,6424	0,6905	0,8766	0,0462	0,4644	0,9123	**0,0098**	0,2739	0,2348
		0,5562	**0,9788**	0,9455	0,9067	0,3862	0,2750	0,8106	0,4349	0,8539	0,7140
		0,1943	0,1659	**0,0231**	0,2165	0,0375	0,4644	0,9216	0,8097	0,7888	0,7497
		0,1981	0,1824	0,1745	0,115	0,0335	0,0874	0,3733	0,9021	0,6550	0,0375
		0,8703	0,8515	0,6917	0,2165	**0,9751**	0,8659	0,6674	0,4470	0,2125	0,7070
		0,1182	0,8499	**0,9857**	0,9704	0,8170	0,8667	0,3631	0,8854	0,5495	0,2125
		0,2245	0,3442	0,5104	0,5881	0,4097	0,4416	0,6259	0,2716	**0,0074**	0,3555
		0,2784	0,1472	0,1285	0,6735	0,3669	0,2165	0,7174	0,0427	**0,0185**	0,6487
		0,4071	0,4084	0,2807	0,7789	0,3979	0,4698	0,7829	0,6637	0,8041	0,9580
		0,5986	0,7023	0,0935	0,8615	0,8394	0,2369	0,9522	0,0459	0,4256	0,4550
		0,7163	0,6078	0,5468	0,9400	0,8152	0,6612	0,9392	0,3028	0,2327	0,1195
		0,0358	0,2627	0,5881	0,5468	0,4914	0,9288	0,6917	0,8419	0,4739	0,2853
		0,3355	0,4901	0,5602	0,3784	0,7023	0,7128	0,1142	0,6104	0,3784	0,3529
		0,2550	0,6662	0,3643	0,1915	0,7518	0,1426	0,1519	0,1815	0,3862	0,3504
		0,2572	0,1543	0,1762	0,4416	0,0333	0,1307	0,2379	0,1004	0,6649	0,9354
		0,4996	0,8484	0,6964	**0,9833**	0,8827	0,1860	0,3656	0,1642	0,0489	0,1209
		0,4045	0,7035	0,3517	0,7355	0,4577	0,7432	0,6038	0,8241	0,2317	0,3631
		0,2705	0,2750	0,2716	0,4150	0,4456	0,3479	0,1897	0,8250	0,5158	0,3479
		0,4363	0,9231	0,5090	0,8223	0,9288	0,5333	0,4955	0,0766	0,3232	0,5828
		0,4032	0,4860	0,8607	**0,9901**	0,5212	0,1418	0,1511	0,6976	0,8814	0,8284
		0,6348	0,3694	0,2165	0,2934	0,1990	0,1373	**0,9979**	0,7582	0,6487	0,4564
		0,7220	0,2096	0,8652	0,7105	0,2887	0,7529	0,2286	0,6845	0,2485	0,4005
		0,1395	0,2307	0,2235	0,9341	0,0482	0,6117	0,0380	0,5212	0,7956	0,5934
		0,3707	0,2672	0,7288	0,2485	0,1433	0,2605	0,4243	0,2485	0,1293	0,6078
		0,5920	0,8188	0,8645	0,5973	0,1952	0,5144	0,4363	0,8344	**0,0208**	0,0427
9	DNA (ДНК)	0,1131	0,0323	0,1097	0,8629	0,6674	0,5548	0,1746	0,8011	0,1278	0,2067
		0,0390	0,5699	0,9731	0,2913	0,8760	0,1708	**0,0134**	0,0791	0,1446	0,0887
		0,7299	0,7280	0,8028	0,6302	0,6566	0,2392	0,8488	0,6978	0,3591	0,2374
		0,1248	0,2550	0,5278	0,5918	**0,9777**	0,3591	0,3181	0,6916	0,2392	0,2665
		0,7936	0,8680	0,4562	0,9344	0,6324	0,0565	0,4550	0,6357	0,6927	0,5278
		0,1064	0,1119	0,8736	0,2355	0,7755	0,7825	0,9106	0,5664	0,1563	0,9047
		0,7040	0,3657	0,6695	0,8609	0,5952	0,8132	0,7181	0,7986	0,5768	0,6369
		0,7415	0,5407	0,3859	0,2374	0,9179	0,4515	0,4503	0,9249	0,3938	0,7328
		0,7444	0,7280	0,3025	0,9096	0,7191	0,4213	0,3492	0,6978	0,9527	0,5687
		0,0181	0,1967	0,0849	0,5536	0,8019	0,7565	0,3938	0,6780	0,6190	0,6168
		0,9677	0,5220	0,4213	0,6313	0,8948	0,3129	0,9115	0,4363	0,8718	0,6043
		0,9963	0,0818	0,9416	0,6490	0,3747	0,1784	0,7319	0,1967	0,2822	0,5571
		0,1716	0,6468	0,6066	**0,9960**	0,4018	0,4075	0,8447	0,4201	0,4973	0,2310
		0,9847	0,0429	0,4410	0,0920	0,1769	0,7885	0,4098	0,8425	0,2041	0,6020
		0,8609	0,5963	0,7111	0,9106	0,7538	0,4305	**0,0207**	0,1831	0,1521	0,5687

N	Название теста	P-value									
		0,0684	0,6674	0,9430	0,7299	0,8249	0,4831	0,3814	0,7666	0,0545	0,8502
		0,4121	0,0827	0,2560	0,0736	0,5606	0,9743	0,9077	0,7270	0,5220	0,5594
		0,8820	0,8036	0,8019	0,3481	0,7519	0,0906	0,7630	0,3171	0,2186	0,0859
		0,6885	0,2627	0,3139	0,0925	0,1599	0,1528	0,5837	0,1855	0,9503	0,0700
		0,0970	0,3098	0,1086	0,7729	0,2248	0,4398	0,8036	0,7141	0,6213	0,3514
		0,1119	0,8418	0,5384	0,4949	0,2852	0,7911	0,5975	0,1086	0,3192	0,7030
		0,8036	0,2169	0,9265	0,4155	0,9175	0,9001	0,3747	0,3635	0,4679	0,4294
		0,3803	0,6716	0,2475	0,5814	**0,0181**	0,0613	0,7729	0,5337	0,5407	0,3266
		0,0642	0,7702	0,9541	0,4679	0,2126	0,2984	0,4259	0,7808	0,4098	0,9580
		0,0504	0,2646	0,3657	0,4550	0,4480	0,2160	0,0940	0,9001	0,0388	0,6077
		0,4937	0,1206	0,1606	0,3927	0,9359	0,8899	0,1406	0,7211	0,0565	0,0708
		0,1426	**0,0064**	0,3234	0,9047	0,1808	0,9440	0,7764	0,8849	0,6885	0,5396
		0,3481	0,2733	0,1086	0,6179	0,0935	0,1694	0,5208	0,3635	0,1967	0,9541
		0,2724	0,4890	0,3780	0,5963	0,9598	0,7808	0,7961	0,4236	0,3558	**0,0143**
		0,0096	0,5803	0,7161	0,6706	0,8019	0,4679	0,3005	0,4456	0,1148	0,2636
		0,0631	0,1620	**0,9766**	0,3569	0,0813	0,4410	0,5126	0,6291	0,7081	0,0661
10	Count the 1's (Подсчет единиц)	0,714894	0,575090	**0,005663**	0,391729	0,399850	0,295492	0,344597	0,173701	0,348327	0,152559
		0,390651	0,677702	0,944315	0,518188	0,432152	0,379694	0,967225	0,287542	0,932459	0,280520
11	Count the 1's for specific bytes (Подсчет единиц для особых байтов)	0,078686	0,028382	0,795949	0,229968	0,967968	0,070933	0,560816	0,551993	0,549646	0,103224
		0,862544	0,405132	0,375743	0,563271	0,867178	0,531178	**0,002915**	0,548852	0,231171	0,740941
		0,910352	0,376152	0,736290	0,277572	0,940202	0,878388	0,544731	**0,980563**	0,527057	0,375656
		0,783577	0,674482	0,342107	0,672611	0,792949	**0,988721**	0,240100	0,953729	0,716548	0,195148
		0,200957	0,557372	0,765765	0,952533	0,954627	0,934087	0,454611	0,828469	0,655336	0,334315
		0,948727	0,637161	0,966979	0,295151	0,289370	0,156322	0,258048	0,645908	0,554291	0,089708
		0,530980	0,172168	0,788793	0,158412	0,890281	0,132731	0,954925	0,526179	0,058457	0,151833
		0,930501	0,479942	0,772539	0,425633	0,398150	0,047034	0,145009	0,792745	0,231758	0,579323
		0,695523	0,460777	0,164707	0,856588	0,262456	0,047144	0,058406	0,456536	0,233515	0,205915
		0,522955	0,412959	0,056288	0,263977	0,115568	0,225058	0,173504	0,193980	0,872040	0,423288
		0,909479	0,248672	0,907020	0,124126	0,232190	0,307111	0,562931	0,638458	0,941000	0,920261
		0,480015	0,692462	0,589969	0,398456	**0,998416**	0,616531	0,548509	0,128201	0,792842	0,086933
		0,573954	0,720346	0,923140	0,032665	0,893723	0,596965	0,679347	0,489554	0,122035	0,268175
		0,545191	0,534033	**0,014472**	0,965313	**0,999707**	**0,021090**	0,838302	0,811093	0,506269	0,615747
		0,399823	0,037942	0,563673	**0,975965**	0,918756	0,839998	0,045193	0,941429	0,905360	0,083975
		0,494548	0,231350	0,072960	0,613148	0,044450	0,940394	0,247920	0,823205	0,301371	**0,022266**
		0,896029	0,030387	0,625825	0,276761	0,856694	0,615897	0,626008	0,523741	**0,987871**	0,573913
		0,427513	0,081480	0,143675	0,386654	0,921515	0,209154	0,461373	0,935504	0,515552	0,220826
		0,247730	0,608265	0,475262	**0,989754**	0,543144	0,207805	0,031024	**0,998059**	0,212846	0,561281
		0,721598	0,381296	0,441191	0,914166	0,836733	0,339288	0,580800	0,573625	0,174684	0,687506
		0,148575	0,307419	0,777024	0,516725	0,220035	0,971262	0,326338	0,828135	0,866283	0,951907
		0,903786	0,694973	0,063373	0,972710	0,723713	0,846615	0,195957	0,534136	0,779790	0,630486
		0,504972	0,663067	0,814942	0,352286	0,850506	0,137501	0,135345	0,946263	0,098587	0,943767
		0,599623	0,497337	0,601925	0,049952	0,035977	0,904354	0,056496	0,855968	0,227193	0,268304
		0,455081	0,905736	0,519484	0,373872	0,160505	0,262129	0,931946	**0,990475**	0,450056	**0,007750**
12	Parking Lot (Парковка)	0,291865	0,939730	0,921543	0,642555	0,819442	0,676028	**0,007758**	0,357445	0,625377	0,100530
		0,219823	0,767486	0,781201	0,136563	0,463618	0,607947	0,117571	0,590298	0,914635	0,518210
		0,030593	0,080965	0,357445	0,078457	0,463618	0,842447	0,085365	0,427537	0,340551	0,676028
		0,307734	0,659449	0,439393	0,934075	0,357445	0,590298	0,853193	0,307734	0,291865	0,374623
		0,218799	0,891189	0,065925	0,150006	0,831196	0,753306	0,899470	0,307734	0,463618	0,842447
		0,642555	0,863437	0,934075	0,232514	0,928066	0,409702	0,572463	0,781201	0,842447	0,536382
		0,374623	0,794438	0,445521	0,427537	0,261324	0,609103	0,030593	0,168804	0,136563	0,033889
		0,014198	0,921543	0,863437	0,723613	0,323972	0,899470	0,918231	0,078457	0,276387	0,374623
		0,100530	0,659449	0,831196	0,518210	0,590298	0,463618	0,831196	0,071432	0,218799	0,232514
		0,041356	**0,975204**	0,873180	0,427537	0,536382	0,659449	0,934075	**0,012629**	0,370627	**0,015932**
		0,218799	0,092718	0,863437	0,157553	0,041356	0,060270	0,831196	0,914635	0,232514	0,973191
13	Minimum Distance (Минимальное расстояние)	0,627269	0,807454	0,347308	0,630934	0,970932	0,311482	0,154158	0,400538	0,229508	0,641902
14	3D-Spheres (3D-Сферы)	0,09773	0,74811	0,83542	0,73944	0,88060	0,45831	0,56057	0,27878	0,15872	0,21294
		0,94238	0,28031	0,05213	0,65822	0,02778	0,27932	0,72907	0,29068	0,14260	0,10230
		0,660568	0,74093	0,55710	0,02749	0,87045	0,66851	0,76466	0,61144	0,17994	0,46675
		0,20752	0,16309	0,15152	0,41626	0,12425	0,05667	0,38906	0,90298	0,13419	0,22466
		0,69941	0,683080	0,60077	0,89238	0,84807	0,62967	0,09201	0,91693	0,54242	**0,98223**
		0,73550	0,19276	0,87524	0,28432	0,49580	0,22844	**0,00447**	**0,01876**	0,11394	0,59112
		0,85447	0,03924	0,556734	0,69310	0,37397	0,70801	0,09732	0,14671	0,33386	0,84485
		0,35185	0,97040	0,81915	0,41373	0,22589	0,52367	0,89622	0,45356	0,17565	0,73981
		0,75863	0,02691	0,84514	**0,019839**	0,47493	0,76008	0,27731	0,34121	0,26244	0,95313
		0,61249	0,50276	0,53815	0,56611	0,63841	0,31482	0,50421	0,27645	0,93708	0,16683
		0,20752	0,88004	0,49056	0,47156	0,596050	0,68377	0,65228	0,55160	0,53927	0,81389
		0,90057	0,42714	0,90867	0,73290	0,85514	**0,00975**	0,76868	0,74609	0,14370	0,66003

N	Название теста	P-value
		0,23831 0,91408 0,56167 0,54537 0,61993 0,922602 0,17996 0,11089 0,82275 0,66127 0,79578 0,77316 0,34934 0,14516 0,45684 0,40941 0,30362 0,42285 **0,01474** 0,49766 0,67109 0,91215 0,68605 0,91869 0,45834 0,40805 0,061860 0,61621 0,21117 0,90446 0,13187 **0,01628** 0,14701 0,26706 0,66047 0,60277 0,37012 0,93392 0,63443 0,72639 0,03432 0,84112 0,64596 0,27449 0,75974 0,05053 0,08818 0,543675 0,84896 0,15406 0,73357 0,13831 0,91181 0,31373 **0,98207** 0,94083 0,49131 0,66189 0,07837 0,04580 0,51564 0,51613 0,17595 **0,99096** 0,48721 0,83958 0,05550 0,20218 0,463039 0,71223 0,30082 0,86757 0,43145 0,21004 0,80087 0,88814 0,13049 0,14904 0,27706 0,77332 0,77229 0,65808 0,89816 0,19899 0,64836 0,34040 0,91775 0,59613 0,03385 0,185831
15	Squeeze test (Тест на сжатие)	0,616762 0,325961 0,900024 0,857510 **0,978950** 0,037271 0,068239 0,603429 0,938010 0,515931
16	Overlapping Sums (Пересекающиеся суммы)	0,864678 0,026302 0,813879 0,281354 0,149326 0,059319 0,250510 0,722141 0,196269 0,630455 0,639839 0,355564 0,808332 0,198394 0,095256 0,674532 0,581517 0,585048 0,119249 0,512568 0,203092 0,489644 0,086434 0,573796 0,361981 0,127168 0,874831 0,631080 0,701629 **0,975436** 0,158588 0,185427 0,132861 0,213850 0,644795 0,338587 0,343997 0,119922 0,720507 **0,009750** 0,608965 0,438330 0,660188 0,567632 0,762113 0,716163 0,814066 0,455273 0,494375 0,390535 0,814928 0,070845 0,910660 0,371088 0,449368 0,669370 0,868768 0,433599 0,363537 0,295522 0,855542 0,917578 0,069872 0,893681 0,151261 0,308443 0,910331 0,452620 0,628842 0,839895 0,872821 0,596257 0,973846 0,949948 0,406781 0,771176 **0,986917** 0,399620 0,049554 0,089040 0,047322 0,593126 0,102408 0,900094 0,138730 0,815456 0,287460 0,924378 0,741905 0,382688 0,463349 0,739512 0,211499 0,175529 0,758220 0,882401 0,870484 0,130904 0,185837 0,049005 0,792653 0,112277 0,073735 0,973033 0,264297 0,066117 **0,992313** 0,434391 0,511284 0,832475
17	Runs (Последовательности)	0,919463 0,785453 0,177584 0,441735 0,865911 0,924968 0,600264 0,114584 0,733124 0,451488 0,164189 0,755491 0,570349 0,635742 0,417154 0,952295 0,454173 0,656935 0,325422 0,903195 0,282056 0,918797 0,102944 0,382095 0,707419 0,754531 0,922808 0,150011 0,049744 **0,978324** 0,480121 0,223959 0,931086 0,357682 0,224279 0,525606 0,494980 0,224138 0,154384 0,131452
18	Craps (Игра в кости)	0,807388 0,160177 0,086361 0,323855 0,572995 0,942894 **0,995328** 0,959789 0,277678 0,293844 0,921969 0,491954 0,693583 0,353810 0,946384 0,960596 0,037950 0,634357 0,335686 0,347650

Для получения окончательного вывода о том, что исследуемый ГПСЧ с успехом прошел тесты, необходимо убедиться, что распределение значений *p-value* соответствует равномерному распределению. Для этого был выбран критерий Пирсона Хи-квадрат (χ^2) как наиболее часто употребляемый критерий для проверки гипотезы о принадлежности наблюдаемой выборки равномерному закону распределения.

Массив из 2200 значений *p-value* был разбит на 10 диапазонов (n = 10), число степеней свободы k = n – 1 = 9. Уровень значимости α = 0,05.

Значение Хи-квадрат вычисляется по формуле:

$$\chi^2 = \sum_{i=1}^{10} \frac{(m_i - m_i')^2}{m_i'}$$

где m_i – эмпирические частоты распределения *p-value* внутри каждого диапазона,

m_i' – теоретические частоты, соответствующие равномерному распределению.

Полученное значение Хи-квадрат сравнивается с табличным критическим при уровне значимости 0,05 и числе степеней свободы 9. Табличное значение Хи-квадрат было получено из программы Microsoft Office Excel (статистическая функция ХИ2ОБР).

Результат проверки приведен в таблице 2.

Массив значений считается удовлетворяющим равномерному распределению, если полученное значение Хи-квадрат меньше табличного. В нашем случае это условие соблюдается.

Таблица 2

N	**Диапазон**	$\mathbf{m_i}$	$\mathbf{m_i'}$	$\mathbf{m_i - m_i'}$	$\frac{(m_i - m_i')^2}{m_i'}$
1	0-0,1	241	220	21	2,004545455
2	0,1-0,2	224	220	4	0,072727273
3	0,2-0,3	240	220	20	1,818181818
4	0,3-0,4	214	220	-6	0,163636364
5	0,4-0,5	215	220	-5	0,113636364
6	0,5-0,6	204	220	-16	1,163636364
7	0,6-0,7	213	220	-7	0,222727273
8	0,7-0,8	182	220	-38	6,563636364
9	0,8-0,9	227	220	7	0,222727273
10	0,9-1	238	220	18	1,472727273
Хи-квадрат рассчитанное					13,81818182
Хи-квадрат табличное					16,91897762

Таким образом, можно сделать вывод о том, что исследованный ГПСЧ с успехом прошел тесты DIEHARD и способен генерировать случайные и независимые числа.

Литература:

1. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness. URL: https://wayback.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/ (последнее обращение: 26.03.2017).

2. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М: КУДИЦ-ОБРАЗ, 2003. 240 с.

3. Статья из Википедии «Тесты diehard». URL: https://ru.wikipedia.org/wiki/Тесты_diehard/ (последнее обращение: 26.03.2017).