ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Департамент программной инженерии

СОГЛАСОВАНО
Зам. директора по работе с НИУ
ООО «1С»

_____ Н.Ю. Старичков
«12» мая 2022г.

УТВЕРЖДАЮ
Академический руководитель
образовательной программы
«Программная инженерия»
профессор департамента
программной инженерии,
канд. техн. наук

_____ В.В. Шилов
«12» мая 2022 г.

КРИПТОГРАФИЧЕСКИ СТОЙКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Программа и методика испытаний

ЛИСТ УТВЕРЖДЕНИЯ

RU.17701729.03.10-01 51 01-1-ЛУ

Исполнитель:
студент группы БПИ201
_____ / Камнев П.А. /
«12» мая 2022 г.

Москва 2022

Инв. № подл	RU.17701729.03.10-01 81 01-1-ПУ
Подп. и дата	
Взам. инв. №	
Инв. № дубл.	
Подп. и дата	

УТВЕРЖДЕН
RU.17701729.03.10-01 51 01-1-ЛУ

КРИПТОГРАФИЧЕСКИ СТОЙКИЙ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Программа и методика испытаний

RU.17701729.03.10-01 51 01-1

Листов 18

Инв. № подл	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
RU.17701729.03.10-01 51 01-1				

Москва 2022

СОДЕРЖАНИЕ

АННОТАЦИЯ

Программа и методика испытаний – это документ, в котором содержится информация о программном продукте, а также полное описание приемочных испытаний для данного программного продукта.

Настоящая Программа и методика испытаний для «Криптографически стойкого генератора псевдослучайных чисел» содержит следующие разделы: «Объект испытаний», «Цель испытаний», «Требования к программе», «Требования к программной документации», «Средства и порядок испытаний», «Методы испытаний».

В разделе «Объект испытаний» указаны наименование, область применения и обозначение испытуемой программы.

В разделе «Цель испытаний» указана цель проведения испытаний.

В разделе «Требования к программе» указаны требования, подлежащие проверке во время испытаний и заданные в техническом задании на проверку.

В разделе «Требования к программным документам» указаны состав программной документации, предъявляемой на испытания, а также специальные требования,

В разделе «Средства и порядок испытаний» указаны технические и программные средства, используемые во время испытаний, а также порядок проведения испытаний.

В разделе «Методы испытаний» приведены описания используемых методов испытаний.

1. ОБЪЕКТ ИСПЫТАНИЙ

1.1. Наименование программы

Полное наименование программы – «Криптографически стойкий генератор псевдослучайных чисел».

1.2. Область применения

Программа, генерирующая последовательности псевдослучайных чисел, которые можно использовать для криптографических целей (например, для генерации ключей).

1.3. Обозначение испытуемой программы

Имя программы: secure-generator.exe

2. ЦЕЛЬ ИСПЫТАНИЙ

Целью проведения испытаний является проверка того, что разработанная программа удовлетворяет функциональным требованиям, статистическим требованиям и требованиям к надежности, перечисленным в разделе «Требования к программе».

3. ТРЕБОВАНИЯ К ПРОГРАММЕ

В рамках испытаний проверяется соответствие программы следующим требованиям, описанным в разделе 4 Технического задания.

3.1. Требования к функциональным характеристикам

3.1.1. Требования к составу выполняемых функций

1. Программа должна позволять генерировать последовательности равномерно распределенных псевдослучайных чисел.
   1.1. Возможно задать промежуток, на котором будут равномерно распределены генерируемые числа.
   1.2. Программа должна позволять генерировать числа в промежутке от 0 до 2^{32} - 1.
2. Программа должна позволять генерировать псевдослучайные последовательности бит.
3. Программа должна позволять инициализировать псевдослучайный генератор как от энтропии устройства, так и от целых чисел от 0 до 2^{32} - 1 (в таком случае каждый раз генерируется одинаковая последовательность).
4. Программа должна позволять выводить генерируемую последовательность как в консоль, так и в файл.
5. Должен присутствовать режим тестирования, позволяющий непрерывно выводить генерируемую последовательность до внешнего завершения процесса.
6. Программа должна запускаться через консоль и позволять задавать через аргументы командной строки параметры генерации псевдослучайных последовательностей.
   6.1. Тип генерируемых значений – числа или биты.
   6.2. При генерации чисел – промежуток, по которому будут равномерно распределены генерируемые числа.
   6.3. Длина генерируемой последовательности. Для генерации чисел – количество чисел, которые будут сгенерированы. Для генерации последовательностей бит – длина псевдослучайной последовательности в байтах.
   6.4. Формат выходных данных – вывод последовательности в консоль или в файл.
   6.5. Имя выходного файла (в случае генерации последовательности в файл).
   6.6. Инициализация псевдослучайного генератора некоторым числом или случайной энтропией, полученной от устройства, на котором происходит запуск.
   6.7. Также должна присутствовать опция тестирования, при наличии которой генератор будет непрерывно выводить последовательность бит в консоль до внешнего завершения процесса.
7. В случае ввода некорректных параметров через аргументы командной строки в консоль выводится информация о том, в каком виде задаются параметры, программа завершает свое выполнение.
8. При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль выводится ошибка, программа завершает свое выполнение.
9. При возникновении ошибок, связанных с получением энтропии от устройства, в консоль выводится краткая информация об ошибке, программа завершает свое выполнение.

3.1.2. Требования к интерфейсу

Взаимодействие пользователя с программой происходит через интерфейс командной строки (консоль).
Запуск генератора через командную строку происходит следующим образом:

secure-generator.exe [опции] [параметры]

Должны быть доступны следующие опции:
- --bits (генерация бит, по умолчанию генерируются числа);
- --min (нижняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^{32} - 1, по умолчанию принимает значение 0;
- --max (верхняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^{32} - 1, по умолчанию принимает значение 2^{32} - 1;
- --length (длина генерируемой последовательности, при генерации чисел – количество чисел, при генерации бит – количество байт), параметром является целое число не менее 1, по умолчанию принимает значение 1;
- --file (вывод в файл, по умолчанию вывод в консоль), параметром является имя файла со сгенерированными значениями, который будет создан в каталоге, где расположен исполняемый файл;
- --seed (инициализировать генератор числом, по умолчанию происходит инициализация энтропией устройства), параметром является целое число в промежутке от 0 до 2^{32} - 1;
- --test_mode (режим тестирования), при выборе этой опции генерируются псевдослучайные биты и непрерывно выводятся в консоль до внешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом.

Пример (генерация 20 псевдослучайных чисел в промежутке от 1 до 10 в файл output.txt):

secure-generator.exe --min 1 --max 10 --length 20 --file output.txt

3.1.3. Требования к организации входных данных

Входными данными являются параметры работы программы, вводимые в виде аргументов командной строки.

3.1.4. Требования к организации выходных данных

В случае вывода генерируемых последовательностей в файл, создается файл с именем, заданным пользователем через аргументы командной строки. В противном случае генерируемые последовательности выводятся в консоль.
- При генерации последовательностей чисел генерируемые числа выводятся через пробел (без дополнительных выходных данных).
- При генерации последовательностей бит происходит вывод двоичных данных (сгенерированные файлы можно просмотреть при помощи специальных редакторов двоичных данных).

3.1.5. Требования к временным характеристикам

Временные характеристики зависят от характеристик устройства, на котором производится тестирования. На устройстве, на котором производится тестирование, время генерации 1 000 000 000 целых чисел в промежутке 0 до 2^{32} - 1 при помощи разрабатываемого

генератора должно превышать не более чем в 10 раз время генерации 1 000 000 000 целых чисел в промежутке 0 до 2^{32} - 1 при помощи встроенного в C++ генератора std::mt_19937.

3.1.6. Требования к статистическим характеристикам

Генерируемые псевдослучайные последовательности должны успешно проходить статистическое тестирование с использованием известной тестовой утилиты PractRand.
Также точки с псевдослучайными координатами, полученными при помощи генератора, при помещении на двумерную плоскость должны равномерно заполнять квадрат (визуальная оценка), углами которого являются точки (a; a) и (b; b), где [a; b] – диапазон генерируемых чисел.

3.2. Требования к математическому обеспечению

В основе псевдослучайного генератора должен лежать алгоритм Hash_DRBG в соответствии со стандартном Национального института стандартов и технологий США NIST SP 800-90A Rev. 1.

3.3. Требования к надежности

Программа должна стабильно работать на компьютере, технические характеристики которого удовлетворяют системным требованиям.

Ошибочные сценарии:

- В случае ввода некорректных параметров через аргументы командной строки в консоль выводится информация о том, в каком виде задаются параметры, программа завершает свое выполнение. Выводимый текст:
  Доступны следующие опции:
  --bits (генерация бит, по умолчанию генерируются числа)
  --min (нижняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 - 1, по умолчанию принимает значение 0
  --max (верхняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 – 1;
  --length (длина генерируемой последовательности, при генерации чисел – количество чисел, при генерации бит – количество байт), параметром является целое число не менее 1, по умолчанию принимает значение 1
  --file (вывод в файл, по умолчанию вывод в консоль), параметром является имя файла со сгенерированными значениями, который будет создан в каталоге, где расположен исполняемый файл
  --seed (инициализировать генератор числом, по умолчанию происходит инициализация энтропией устройства), параметром является целое число в промежутке от 0 до 2^32 - 1
  --test_mode (режим тестирования), при выборе этой опции генерируются псевдослучайные биты и непрерывно выводятся в консоль до внешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом (--seed)
- При использовании несовместимых опций (--bits и --min или --max, --test_mode и любая другая опция, кроме --seed) выводится ошибка. Шаблон ошибки:
  Использованы несовместимые опции <опция 1> и <опция 2>.
- Если указана опция, но не указан ее параметр (кроме --bits и –test_mode), выводится ошибка по шаблону:
  Не указан параметр для опции <опция>.

- При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль выводится ошибка, программа завершает свое выполнение. Текст ошибки:
  На диске недостаточно свободного места для генерации значений в файл. Проверьте параметр --length.
- При возникновении ошибок, связанных с получением энтропии от устройства, в консоль выводится краткая информация об ошибке, программа завершает свое выполнение. Текст ошибки:
  Возникла ошибка при получении энтропии от устройства. Проверьте соответствие системным требованиям.

3.4. Требования к информационной и программной совместимости

3.4.1. Требования к исходным кодам и языкам программирования

Программа должна быть написана на языке C++17.
В исходном коде программы разрешается использовать:

- стандартную библиотеку языка C++;
- библиотеку OpenSSL с открытым исходным кодом;
- WinAPI и Microsoft CryptoAPI;

4. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

4.1. Состав программной документации

1. «Криптографически стойкий генератор псевдослучайных чисел». Техническое задание (ГОСТ 19.201-78).
2. «Криптографически стойкий генератор псевдослучайных чисел». Программа и методика испытаний (ГОСТ 19.301-78).
3. «Криптографически стойкий генератор псевдослучайных чисел». Пояснительная записка (ГОСТ 19.404-79).
4. «Криптографически стойкий генератор псевдослучайных чисел». Руководство оператора (ГОСТ 19.505-79).

4.2. Специальные требования к программной документации

Документы к программе должны быть выполнены в соответствии с ГОСТ 19.106-78 и ГОСТами к каждому виду документа (см. п. 5.1.);

Пояснительная записка должна быть загружена в систему Антиплагиат через LMS «НИУ ВШЭ».

Документация и программа сдаются в электронном виде в формате .pdf или .docx. в архиве формата .zip или .rar;

За один день до защиты комиссии все материалы курсового проекта:

– техническая документация,
– программный проект,
– исполняемый файл,
– отзыв руководителя,
– лист Антиплагиата

должны быть загружены одним или несколькими архивами в проект дисциплины «Курсовой проект 2021-2022» в личном кабинете в информационной образовательной среде LMS (Learning Management System) НИУ ВШЭ.

5. СРЕДСТВА И ПОРЯДОК ИСПЫТАНИЙ

5.1. Технические средства, используемые во время испытаний

Рекомендуемые минимальные параметры устройства для проведения полноценного тестирования программы:

- процессор с частотой не менее 1 ГГц;
- 2 ГБ оперативной памяти;
- 20 ГБ свободного места на диске;
- клавиатура;
- видеоадаптер DirectX 9 или более поздняя версия с драйвером WDDM 1.0 и монитор с разрешением Super VGA (800 x 600).

5.2. Программные средства, используемые во время испытаний

Необходимое ПО для полноценного тестирования программы:

- операционная система Windows 10 64-разрядная;
- Microsoft Visual Studio 2017;
- Microsoft Office Excel;
- пакет PractRand (тестовая утилита);

5.3. Порядок проведения испытаний

Испытания программы должны проводиться в следующем порядке:

1) Проверка требований к программной документации
2) Проверка требований к интерфейсу (базовый запуск программы)
3) Проверка требований к функциональным характеристикам
4) Проверка требований к статистическим характеристикам

6. МЕТОДЫ ИСПЫТАНИЙ

6.1. Испытание выполнения требований к программной документации

Состав программной документации проверяется визуально, проверяется наличие всех подписей и наличие программной документации в системе LMS. Также визуально проверяется соответствие документации требованиям ГОСТ. Все документы удовлетворяют представленным требованиям.

6.2. Проверка требований к интерфейсу. Запуск программы

Действия, необходимые для запуска утилиты, описаны в документе «Криптографически стойкий генератор псевдослучайных чисел. Руководство оператора»

Утилита должна корректно запускаться в режиме интерфейса командной строки.

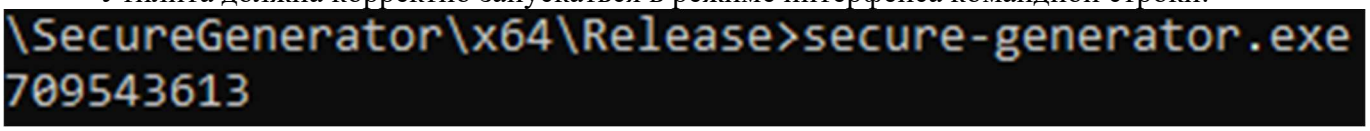

Рисунок 1. Запуск утилиты генерации в режиме командной строки

6.3. Проверка требований к функциональным характеристикам

6.3.1. Генерация последовательностей псевдослучайных чисел

С использованием опции --length можно сгенерировать несколько псевдослучайных чисел. Числа должны находиться в диапазоне от 0 до $2^{32} – 1$.

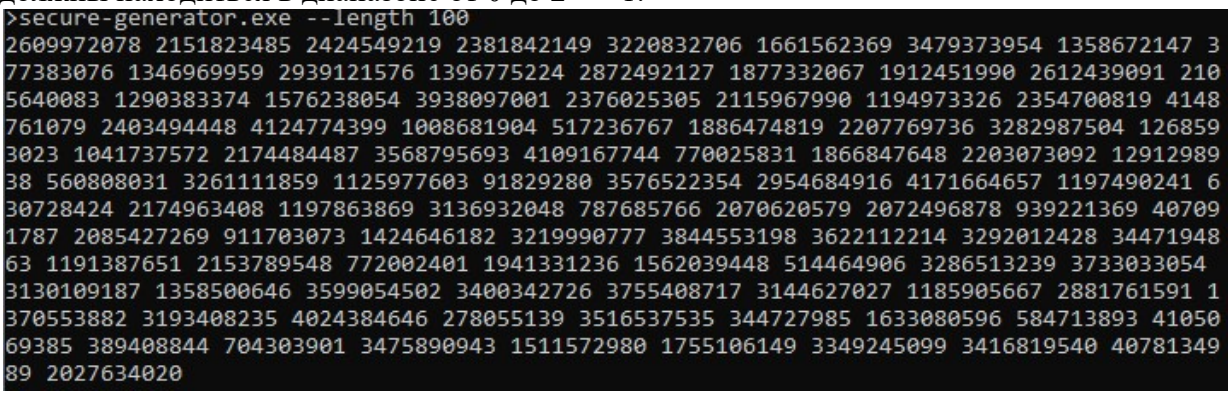

Рисунок 2. Генерация последовательности из нескольких псевдослучайных чисел

6.3.2. Инициализация генератора от энтропии устройства и от целого числа

При инициализации генератора без опции --seed происходит инициализация генератора от энтропии устройства – генерируемые последовательности должны каждый раз отличаться.

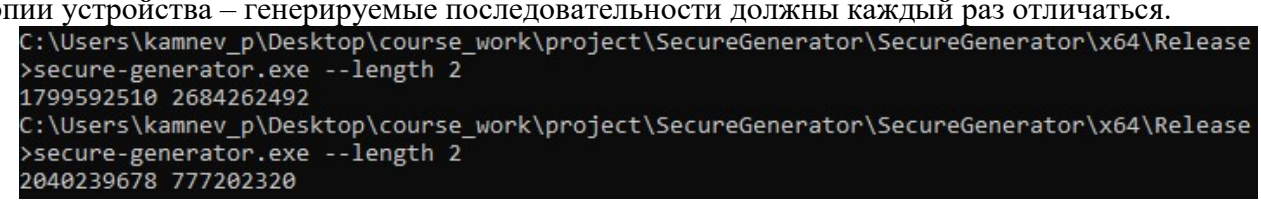

Рисунок 3. Инициализация генератора энтропией устройства

Если использовать опцию --seed, при одинаковом значении параметра генератор каждый раз должен генерировать одну и ту же последовательность.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2 --seed 1
151440905 1449946105
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release
>secure-generator.exe --length 2 --seed 1
151440905 1449946105
```

Рисунок 4. Инициализация генератора одним и тем же числом

6.3.3. Вывод генерируемых последовательность в консоль и в файл

При использовании опции --file <имя> в папке с исполняемым файлом должен появляться файл <имя>, содержащий сгенерированную последовательность

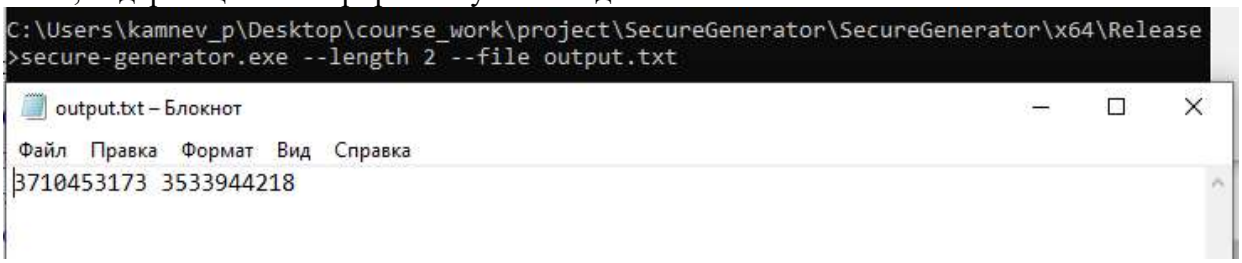

Рисунок 5. Генерация значений в файл

6.3.4. Генерация битовых последовательностей

При использовании опции --bits генерируемые значения должны быть байтовыми. Открыть бинарный файл можно при помощи Hex Editor Neo.

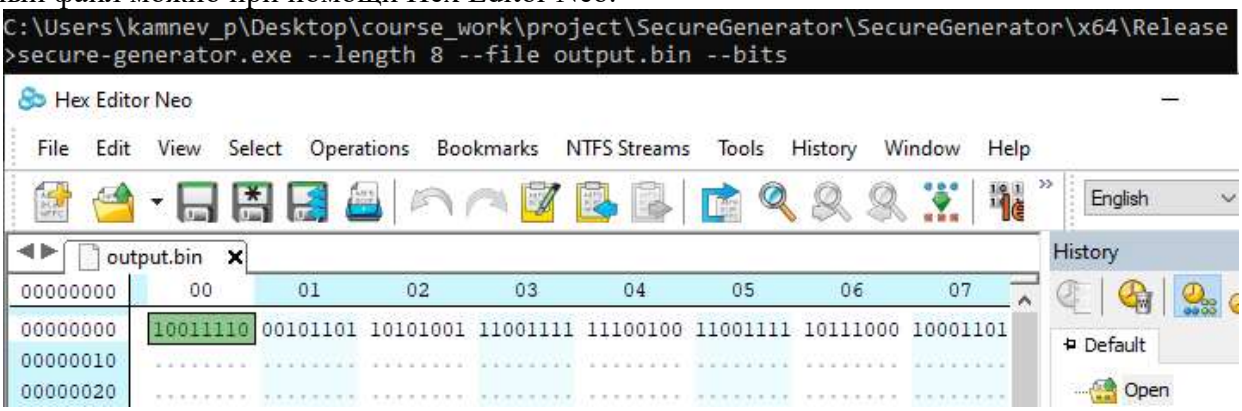

Рисунок 6. Генерация битовых псевдослучайных данных

6.3.5. Генерация чисел в заданном промежутке

Опции --min и --max позволяют задавать минимальное и максимальное значение генерируемых чисел. При их использовании числа должны находиться в заданном промежутке.

```
>secure-generator.exe --length 10 --min 1 --max 10
10 7 5 9 8 9 2 8 4 6
```

Рисунок 7. Генерация чисел в заданном промежутке

6.3.6. Задание длины псевдослучайной последовательности

С использованием опции --length [длина] можно сгенерировать несколько псевдослучайных чисел. Длина последовательности должна совпадать параметру [длина].

```
>secure-generator.exe --length 10 --min 1 --max 10
10 7 5 9 8 9 2 8 4 6
```

Рисунок 8. Задание длины псевдослучайной последовательности

6.3.7. Опция тестирования

При использовании опции --test_mode утилита должна начать выводить сырой поток бит в консоль. Генератор должен успешно проходить тестирование при помощи тестовой утилиты PractRand (вплоть до объема 32TB и далее).

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe --test_mode |
 .\..\..\..\PractRand_094\bin\msvc12_64bit\RNG_test.exe stdin
RNG_test using PractRand version 0.94
RNG = RNG_stdin, seed = unknown
test set = core, folding = standard(unknown format)

rng=RNG_stdin, seed=unknown
length= 128 megabytes (2^27 bytes), time= 2.7 seconds
  no anomalies in 196 test result(s)

rng=RNG_stdin, seed=unknown
length= 256 megabytes (2^28 bytes), time= 5.8 seconds
  no anomalies in 213 test result(s)

rng=RNG_stdin, seed=unknown
length= 512 megabytes (2^29 bytes), time= 11.4 seconds
  no anomalies in 229 test result(s)

rng=RNG_stdin, seed=unknown
length= 1 gigabyte (2^30 bytes), time= 22.4 seconds
  no anomalies in 248 test result(s)

rng=RNG_stdin, seed=unknown
length= 2 gigabytes (2^31 bytes), time= 44.0 seconds
  no anomalies in 266 test result(s)
```

Рисунок 9. Режим тестирования

6.3.8. Вывод ошибок

В случае ввода некорректных параметров через аргументы командной строки в консоль должна выводиться информация о том, в каком виде задаются параметры, программа завершает свое выполнение.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\x64\Release>secure-generator.exe --distribution
Доступны следующие опции:
--bits (генерация бит, по умолчанию генерируются числа)
--min (нижняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 - 1, по умолчани
ю принимает значение 0
--max (верхняя граница промежутка генерируемых чисел), параметром является целое число в промежутке от 0 до 2^32 – 1;
--length (длина генерируемой последовательности, при генерации чисел – количество чисел, при генерации бит – количество байт), п
араметром является целое число не менее 1, по умолчанию принимает значение 1
--file (вывод в файл, по умолчанию вывод в консоль), параметром является имя файла со сгенерированными значениями, который будет
 создан в каталоге, где расположен исполняемый файл
--seed (инициализировать генератор числом, по умолчанию происходит инициализация энтропией устройства), параметром является цело
е число в промежутке от 0 до 2^32 - 1
--test_mode (режим тестирования), при выборе этой опции генерируются псевдослучайные биты и непрерывно выводятся в консоль до вн
ешнего завершения процесса, единственная доступная опция при наличии данного параметра – инициализация числом (--seed)
```

Рисунок 10. Неправильный параметр

При использовании несовместимых опций (--bits и --min или --max, --test_mode и любая другая опция, кроме --seed) должна выводиться ошибка.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe --bits --min 2

Использованы несовместимые опции --bits и --min.
```

Рисунок 11. Использование несовместимых опций

Если указана опция, но не указан ее параметр (кроме --bits и –test_mode), должна выводиться ошибка.

```
>SecureGenerator.exe --min
Не указан параметр для опции --min
```

Рисунок 12. Не указан параметр для опции

При генерации значений в файл программа проверяет доступное место на диске. Если места на диске недостаточно, в консоль должна выводиться ошибка, программа завершает свое выполнение.

```
C:\Users\kamnev_p\Desktop\course_work\project\SecureGenerator\SecureGenerator\Release>SecureGenerator.exe
 --file out --length 1000000000000000
На диске недостаточно свободного места для генерации значений в файл. Проверьте параметр --length.
```

Рисунок 13. На диске недостаточно места для генерации значений в файл

6.4. Проверка требований к статистическим характеристикам

Генерируемые псевдослучайные последовательности должны успешно проходить статистическое тестирование с использованием известной тестовой утилиты PractRand на объемах данных 32ТБ и больше:

rng=RNG_stdin, seed=unknown
length= 32 terabytes (2^45 bytes), time= 397777 seconds
no anomalies in 458 test result(s)

Также точки с псевдослучайными координатами, полученными при помощи генератора, при помещении на двумерную плоскость должны равномерно заполнять квадрат (визуальная оценка), углами которого являются точки (a; a) и (b; b), где [a; b] – диапазон генерируемых чисел. График можно построить при помощи Microsoft Excel.

Сгенерируем 10000 двумерных точек с координатами x и y на промежутке от 0 до UINT32_MAX, построим график:

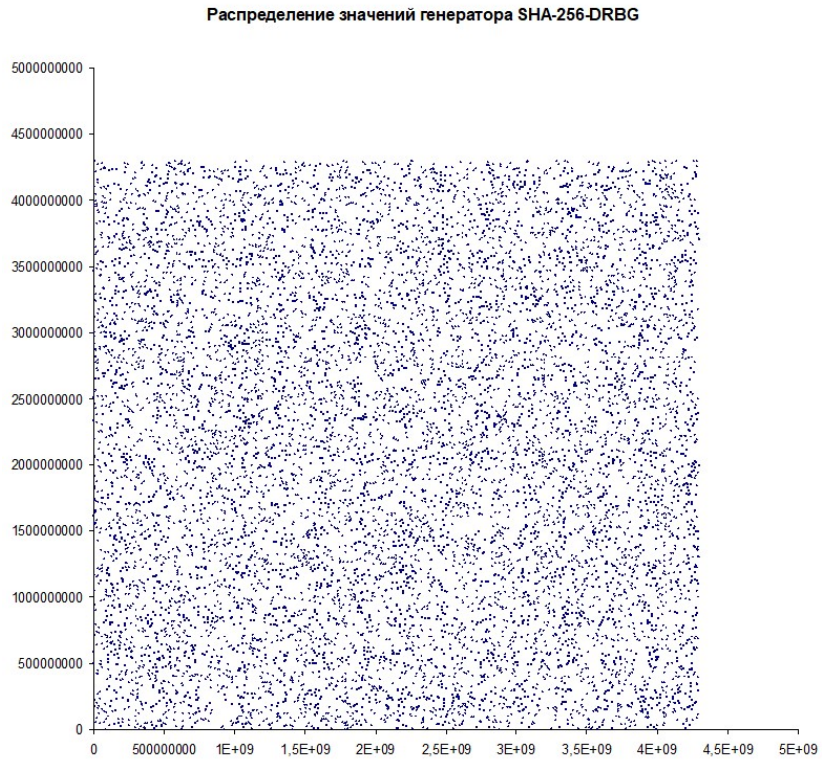

Рисунок 14. Распределение 10000 псевдослучайных точек

Построим более плотный график уже с 20000 точками:

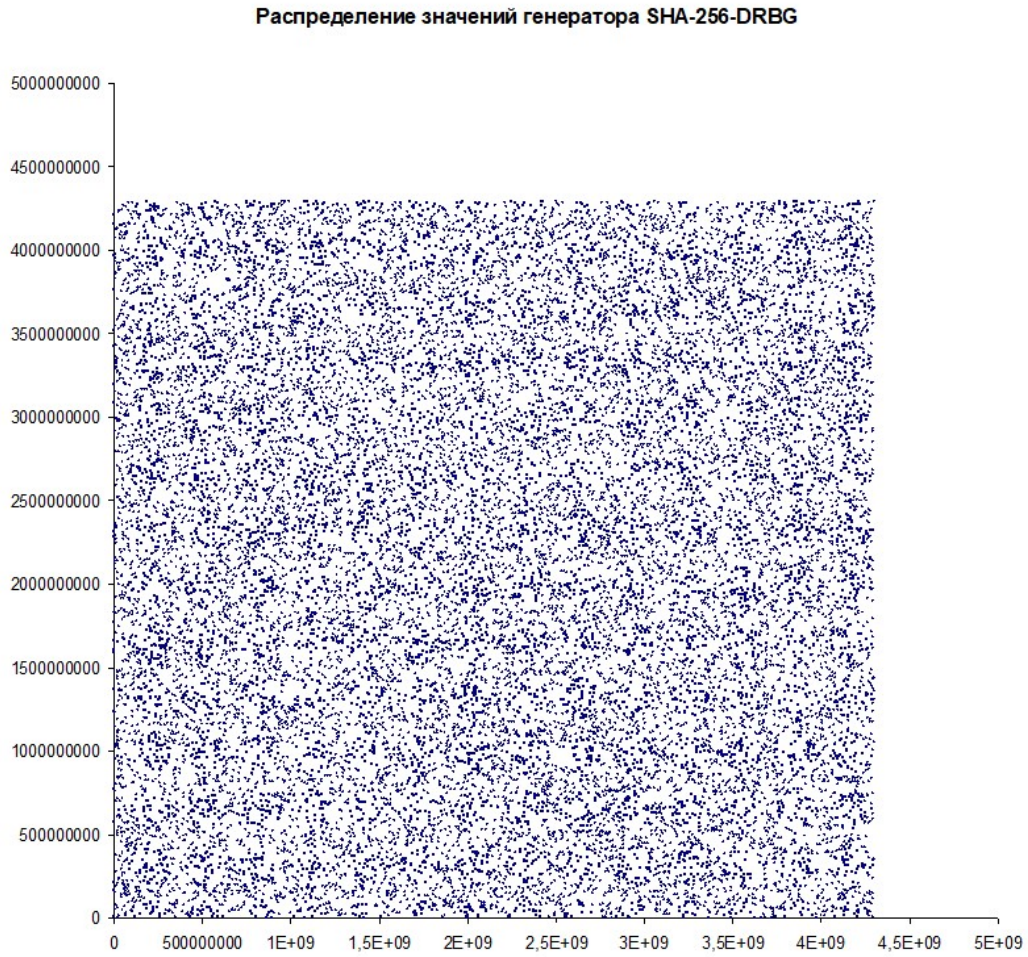

Рисунок 15. Распределение 20000 псевдослучайных точек

Визуально распределение должно выглядеть, как случайное – паттернов не заметно.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц в докум.)	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	Измененных	Заменен ных	Новых	Аннулированных					

Изм.	Лист	№ докум.	Подп.	Дата
RU.17701729.03.10-01 51 01-1				
Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата