

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет информационных технологий и робототехники

Кафедра «Программное обеспечение информационных систем и технологий»

ДОПУЩЕН К ЗАЩИТЕ

Заведующий кафедрой

  
(подпись)

Ю.В. Полозков  
(инициалы и фамилия)

« 13 » 06 2019 г.

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
ДИПЛОМНОГО ПРОЕКТА**

**«Моделирование и тестирование физического генератора случайных чисел»**

Специальность 1-40 01 01 «Программное обеспечение информационных технологий»  
Специализация 1-40 01 01 05 «Управление качеством и тестирование программного обеспечения»

Обучающийся

группы 30701214  
(номер)

Руководитель

Консультанты:

по компьютерному проектированию

по разделу «Охрана труда»

по разделу «Экономика»

Ответственный за нормоконтроль

Объем проекта:

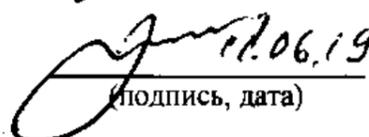
расчетно-пояснительная записка – 62 страниц;

графическая часть – 5 листов;

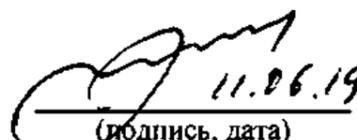
магнитные (цифровые) носители – 1 единиц.

  
(подпись, дата)

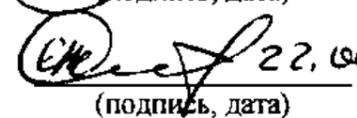
Д.В. Туровский

  
(подпись, дата)

Н.А. Разоренов

  
(подпись, дата)

Н.А. Разоренов

  
(подпись, дата)

А.М. Лазаренков

  
(подпись, дата)

И.В. Насонова

  
(подпись, дата)

Н.С. Домаренко

## РЕФЕРАТ

### ФИЗИЧЕСКИЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ, КОЛЬЦЕВОЙ ОСЦИЛЛЯТОР, ФИЗИЧЕСКАЯ МОДЕЛЬ, ЛОГИЧЕСКАЯ МОДЕЛЬ, ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Объектом исследования являются случайные последовательности чисел.

Цель проекта – смоделировать генератор случайных чисел, отвечающий современным криптографическим требованиям, для дальнейшего использования данной модели в физическом устройстве.

В процессе работы (проектирования) выполнены следующие исследования (разработки): разработаны логическая и физическая модели функционирования приложения; написаны тесты для изучения качества получаемых случайных последовательностей; созданы тесты для критического и углубленного тестирования приложения; спроектирован пользовательский интерфейс.

Элементами научной значимости полученных результатов являются использованные в работе методы и способы генерации равномерно распределенных случайных последовательностей.

Практическая значимость исследования заключается в возможности использовать полученные результаты в конструировании физического устройства, и дальнейшем его применении в криптографии, науке и игровых приложениях.

В ходе дипломного проектирования прошли апробацию такие предложения, как создание приложения для генерации случайных последовательностей.

Результатами внедрения явились: разработка приложения для генерации случайных последовательностей.

Студент-дипломник подтверждает, что приведенный в дипломном проекте расчетно-аналитический материал объективно отражает состояние исследуемого процесса (разрабатываемого объекта), все заимствованные из литературных и других источников теоретические и методологические положения и концепции сопровождаются ссылками на их авторов.

Дипломный проект: 62 с., 8 рис., 21 табл., 11 источников, 1 прил.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Pisarenko I. Neural network technologies in security – Journal of Information Security. № 4, 2009.
2. Scott A. Vanstone Alfred J. Menezes, Paul C. van Oorschot. HandBook of Applied Cryptography. – CRC Press, August 2001.
3. Viktor Fischer, Nathalie Bochard, Florent Bernard and Boyan Valtchanov. True-randomness and pseudo-randomness in ring oscillator-based true randomnumber generators. International Journal of Reconfigurable Computing, 2010:13, 2010.
4. STMicroelectronics. STM32F Datasheet. – DocID15818 Rev 11. Nov.2013.
5. Microsoft Visual Studio, Wikipedia [Электронный ресурс]. – Режим доступа: [https://ru.wikipedia.org/wiki/Microsoft\\_Visual\\_Studio](https://ru.wikipedia.org/wiki/Microsoft_Visual_Studio). Дата доступа: 04.04.2019.
6. C Sharp, Wikipedia [Электронный ресурс]. – Режим доступа: [https://ru.wikipedia.org/wiki/C\\_Sharp](https://ru.wikipedia.org/wiki/C_Sharp). Дата доступа: 04.04.2019.
7. Elaine Barker and John Kelsey. Recommendation for the Entropy Sources Used for Random Bit Generation. – NIST DRAFT Special Publication 80090B, 2012.
8. Максимов Г.Т. Техничко-экономическое обоснование дипломных проектов: Метод. пособие для студентов всех спец. БГУИР дневной и заочной форм обучения. В 4 ч. Ч. 1. Научно-исследовательские проекты / Г.Т. Максимов. – Мн.: БГУИР, 2003. – 44 с.: ил.
9. Санитарные нормы и правила «Требования при работе с видеодисплейными терминалами и электронно-вычислительными машинами» и Гигиенический норматив «Предельно-допустимые уровни нормируемых параметров при работе с видеодисплейными терминалами и электронно-вычислительными машинами», утвержденные постановлением МЗ РБ от 28.06.2013 г. № 59.
10. Лазаренков, А.М. Охрана труда в машиностроении: учебное пособие / А. М. Лазаренков. – Минск: ИВЦ Минфина, 2017. – 446 с.
11. Лазаренков А.М., Ушакова И.Н. Охрана труда: Учебно-методическое пособие для практических занятий. – Мн.: БНТУ, 2011. – 205 с.