Национальный исследовательский ядерный университет «МИФИ»

Факультет Кибернетики и информационной безопасности

Кафедра «Компьютерные системы и технологии»

**Техническое задание**

на учебно-исследовательскую работу (курсовое проектирование)

Студенту гр.

**Тема:**

Повышение эффективности графических тестов для исследования результатов стохастических преобразований

Содержание технического задания:

Основную роль в решении задач защиты информации играют так называемые стохастические методы защиты, то есть методы, прямо или косвенно основанные на использовании генераторов псевдослучайных последовательностей (ГПСП) или хеш-генераторов. Псевдослучайная последовательность (ПСП) по своим свойствам неотличима от истинно случайной последовательности, но в отличие от последней ее можно повторить, и этот факт делает ГПСП неотъемлемым элементом любой системы защиты. Соответственно, тестирование ГПСП является актуальной задачей. Системы тестирования могут содержать оценочные и графические тесты. Оценочные тесты возвращают результат своей работы в виде численной статистики. Графические же тесты позволяют увидеть общую картину, а кроме того, позволяют выявить статистические слабости, не обнаруживаемые оценочными тестами. Также графические тесты могут использоваться для оценки изменений, вносимых нелинейными преобразованиями, а также оценки автокорреляции и корреляции между последовательностями.

Для реализации программного средства тестирования ГПСЧ, необходимо:

1. Изучить методы графического тестирования псевдослучайных последовательностей.
2. Провести обзор и анализ методов улучшения графических тестов.
3. Разработать архитектуру системы и графический интерфейс пользователя.
4. Реализовать программное обеспечение с оригинальными и улучшенными тестами.
5. Провести тестирование и отладку разработанного программного средства.
6. Представить отчёт о проведённой работе и исходный код разработанного программного средства.

**Литература**

1. M.A. Ivanov and I.V. Chugunkov, Theory, application and assessment of the quality of pseudorandom sequences generators. Мoscow: KUDITS-OBRAZ, 2003, 240 p.
2. I.V. Chugunkov and Muleys R.B “Pseudorandom numbers generators quality assessment using graphic tests” in Proc. IEEE North West Russia Young Researchers in Electrical and Electronic Engineering Conf., St. Petersburg, 2014, pp. 8-13.
3. I.V. Chugunkov. Methods and tools to evaluate the quality of pseudorandom sequences generator, focused on solving information security problems. Moscow: NRNU MEPHi, 2012, 236 p.

Место выполнения: Кафедра 12 НИЯУ МИФИ

Дата выдачи задания < >\_\_\_\_\_\_\_\_\_\_\_\_\_2016 г.

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Прокофьев А.О./

Задание принял к исполнению: \_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_ /

**Отзыв о работе студента**

Руководитель \_\_\_\_\_\_\_\_\_\_\_ < >\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2016 г.