Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

КАФЕДРА

Прикладной математики и кибернетики

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
МАГИСТРАНТА

СТУДЕНТА Чусовитин А.Р ГРУППЫ МГ-172

УТВЕРЖДАЮ

«20» января 2019 г.

Зав. Кафедрой

/ А.Н Фионов /

Новосибирск 2019 г.

1. Тема выпускной квалификационной работы магистранта

Реализация и исследование поточного шифра на основе алгоритма Шеннона

утверждена приказом СибГУТИ от «01» октября 2017 г. № 4/1208о-1-1

2.Срок сдачи студентом законченной работы « 25 » июня 2019 г.

3.Исходные данные к работе

1 Ryabko, B. (2018). Properties of two Shannon's ciphers. Designs, Codes and Cryptography, 86(5), 989-995

2 Ракитский А.А., Чусовитин А.Р.Поточный шифр на основе шифра Шеннона // XVI Российская конференция "Распределенные информационно-вычислительные рессурсы. Наука - цифровой экономике" (DICR-2017). 4-7 декабря 2017, ИВТ СО РАН, г. Новосибирск. (РИНЦ)

3 Е.В. Игоничкина Статистический анализ поточных шифров //https://cyberleninka.ru/article/v/statisticheskiy-analiz-potochnyh-shifrov

4.Содержание пояснительной записки (перечень подлежащих разработке вопросов)	**Сроки выполнения по разделам**
Введение	18.01.19-05.02.19г.
Изучение свойств и реализации шифра RC-4	05.02.19-05.03.19г.
Реализация криптосистемы на основе алгоритма Шеннона	06.03.19-14.03.19г.
Изучения свойств реализации	15.03.19-10.05.19г.
Сравнительный анализ поточных шифров RC-4 и реализации алгоритма Шеннона	10.05.19-01.06.19г.
Заключение	05.06.19-16.06.19г.

Дата выдачи задания « 20 » января 2019 г.

Руководитель _____

подпись

Задание принял к исполнению « 20 » января 2019 г.

Студент _____

подпись

АННОТАЦИЯ

Выпускная квалификационная работа Чусовитина Антона Романовича
(Фамилия,И.О.)
по теме «Реализация и исследование поточного шифра на основе алгоритма Шеннона»

Объём работы - *33* страницы, на которых размещены 5 рисунков и 5 таблиц. При написании работы использовалось *9* источников.

Ключевые слова: алгоритм Шеннона, идеальная криптосистема, поточный шифр.

Работа выполнена на Кафедре ПМиК
СибГУТИ Руководитель – к.т.н.,
доцент, А.А. Ракитский

Цель работы: Реализовать и исследованы свойства криптосистемы на основе алгоритма Шеннона. Проведено сравнение скорости шифрования с текущем стандартом RC-4. Также изучены практические статистические показатели алгоритма Шеннона. Изучено влияние количества шифруемых файлов на статистические свойства шифртекста.