Федеральное агентство связи

Федеральное государственное бюджетное образовательное

учреждение

высшего образования

«Сибирский государственный университет телекоммуникаций и

информатики»

(СибГУТИ)

Форма утверждена научно-методическим

советом университета

протокол № 4 от 18.03.2008 г.

**РЕЦЕНЗИЯ**

**на магистерскую диссертацию**

Студента Чусовитина Антона Романовича

По специальности (группа, шифр) 09.04.01 «Информатика и вычислительная техника». Группа «МГ-172»

Тема магистерской диссертации «Реализация и исследование поточного шифра на основе алгоритма Шеннона»

Объем диссертации 43 страницы, на которых размещены 5 рисунков и 5 таблиц.

Заключение о степени соответствия выполненной работы техническому

заданию. В представленной работе подробно описана реализация криптосистемы на основе алгоритма Шеннона. Проведены и описаны статистические тесты для шифруемых последовательностей рассматриваемым алгоритмом и проведено сравнение по скорости шифрования с текущим стандартом RC-4. Работа выполнена в соответствии с поставленным заданием.

Характеристика выполнения основных разделов работы, качество расчетов,

конструктивных решений, практического подтверждения

В представленной диссертации описаны теоретические свойства алгоритма Шеннона и сравниваемого с ним шифра RC-4. Подробно описана рассматриваемая реализация и теоретически доказаны свойства криптосистемы. Параметры криптосистемы являются логичными и обоснованными автором. Итоговые результаты подтверждены экспериментальными исследованиями.

Научная ценность работы

Проведено исследование реализации криптосистемы для доказательства теоретических свойств алгоритма в современных криптосистемах. Проведены сравнительные испытания для сравнения с текущим стандартом поточного шифрования RC-4.

Общая грамотность, качество оформления текста Диссертационная работа оформлена в соответствии со стандартами, предъявляемыми к выпускным квалификационным работам магистров.

Перечень положительных качеств диссертации

Приведены качественное теоретическое обоснование шифра. Обоснованы теоретически и проверены экспериментально статистические свойства зашифрованных последовательностей шифром Шеннона. Работа имеет научную и практическую ценность доказывающую возможность применения шифра Шеннона на практике в современных криптосистемах.

Основные замечания и недостатки диссертации. В работе автора не хватает рисунков, иллюстрирующих работу криптосистемы.

Предполагаемая оценка работы ОТЛИЧНО

Рецензент доцент кафедры ВС, к.т.н Ефимов Александр Владимирович

24.06.2019

(должность, уч. степень, подпись, фамилия, имя, отчество (полностью), дата)