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 Анискиной Алисы Денисовны

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

Тема магистерской диссертации: «Исследование и анализ надёжности шифра Шеннона»

Объем диссертации: 40 страниц

Заключение о степени соответствия выполненной работы техническому заданию: В представленной диссертации подробно рассмотрены атаки и методы исследования криптостойкости поточных шифров, описан и проанализирован шифр Шеннона, рассмотрены возможности проведения атак на рассматриваемый шифр. Содержание диссертационной работы полностью соответствует техническому заданию.

Характеристика выполнения основных разделов работы, качество расчетов, конструктивных решений, практического подтверждения: В диссертационной работе рассматриваются криптографические атаки, применяемые к поточным шифрам, приводятся публикации, в которых атаки применялись на практике, рассмотренные атаки исследуются на возможность применения к шифру Шеннона. В пятой, шестой и седьмой главе подробно описаны этапы тестирования шифра при помощи различных методик, результаты исследований представлены в виде графиков, на основе полученных при анализе данных сделаны выводы о свойствах шифра. Выбор методов исследования имеет чёткое теоретическое обоснование, итоговые результаты проведённого анализа подтверждаются многочисленными экспериментальными исследованиями.

Научная ценность работы: проведено исследование криптостойкости реализации шифра на основе алгоритма Шеннона, исходя из результатов тестирования были проанализированы свойства шифра, сформированы его достоинства и недостатки, сделан вывод о надежности алгоритма.

Общая грамотность, качество оформления текста: Диссертационная работа оформлена грамотно и соответствует всем требованиям, предъявляемым к выпускным квалификационным работам магистров.

Перечень положительных качеств диссертации: В работе представлен качественный теоретический анализ практической реализации шифра Шеннона. Кроме того, было проведено экспериментальное исследование шифра на устойчивость к разного вида атакам. Проведённый анализ является невероятно важным для возможности применения шифра Шеннона на практике, так как шифр является новым и слабо исследованным.

Основные замечания и недостатки диссертации: В работе недостаёт наглядности рассматриваемым атакам, не хватает качественных и подробных иллюстраций, демонстрирующих во всех деталях взаимодействие злоумышленника с шифрующей системой.

Предполагаемая оценка работы:

Рецензент

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