

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Уральский технический институт связи и информатики (филиал) ФГБОУ ВО
«Сибирский государственный университет телекоммуникаций и информатики»
в г. Екатеринбурге
(УрТИСИ СибГУТИ)

направление подготовки (специальность) 09.03.01 «Информатика и вычислитель-
-ная техника»

направленность (профиль)/специализация «Программное обеспечение средств
вычислительной техники и автоматизированных систем»

АННОТАЦИЯ

Выпускной квалификационной работы обучающегося
Дугаря Николая Сергеевича

(ФИО обучающегося(ихся))

на тему

Разработка протокола шифрования на основе сети Фейстеля и схем Лая-Мэсси

Объём работы – 55 страниц, на которых размещено 33 рисунка.

При написании работы использовалось 15 источников.

Ключевые слова:

протокол, структура, сеть, схема, Фейстеля, Лая, Мэсси, функция, метод,
алгоритм, шифрование, зашифрование, расшифрование, шифр, блок, полублок,
открытый текст, шифртекст, данные, информация, криптография,
криптографический, данные, информация, бит, байт, Диффи, Хеллман.

Работа выполнена в соответствии с техническим заданием

Руководитель Адилъ Ильмирович Бурумбаев
(Ф.И.О.)

Целью работы являлось:

Разработка протокола шифрования на основе сети Фейстеля и схем Лая-Мэсси

Решаемые задачи:

Изучение объекта исследования, проектирование структуры шифра на основе
сети Фейстеля и схем Лая-Мисси, выбор технологий для программной реализации

шифра, практическая реализация программного продукта в виде модуля зашифрования, тестирование программного продукта, выводы о безопасности разработки и эксплуатации программного продукта

Основные результаты:

В ходе выполнения выпускной квалификационной работы удалось разработать структуру шифра на основе сети Фейстеля и схем Лая-Мэсси. Тестирование шифра показало недостаточный уровень энтропии выходных шифртекстов.