БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Ручные протоколы аутентификации и секретных вычислений»

Сидорчик Виктория Адамовна

Научный руководитель – кандидат физ.-мат. наук Агиевич С.В.

Минск, 2018

Реферат

Отчет по дипломной работе, 47 с., 6 табл., 15 рис., 10 источников.

Ключевые слова – РУЧНЫЕ ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ, ЛАТИНСКИЕ КВАДРАТЫ.

Объект исследования – ручные протоколы, латинские квадраты.

Цель работы – провести анализ известных ручных протоколов аутентификации и секретных вычислений, разработать ручной протокол на основе латинских квадратов.

Методы исследования – чтение и анализ литературы, сравнение различных протоколов, неполная индукция, методы комбинаторного анализа.

Результаты – были исследованы известные протоколы аутентификации и ручные секретные вычисления, разработан ручной протокол на основе латинских квадратов.

Область применения: криптография, протоколы аутентификации.

Abstract

Report on the degree work, 47 p., 6 tables, 15 figures, 10 sources.

Keywords – HUMAN IDENTIFICATION PROTOCOLS, LATIN SQUARES.

The object of study – human identification protocols, latin squares.

The purpose of the work – analyze human identification protocols and secret calculations, develop human identification protocols based on Latin squares.

Research methods – reading and analysis of literature, comparison of various protocols, incomplete induction, methods of combinatorial analysis.

Results – known human identification protocols s and secret calculations were investigated, a human protocol based on Latin squares was developed.

Application area – cryptography, authentication protocols.