МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

ДРУЩИЦ

Алексей Владимирович

ПОСТРОЕНИЕ И ОЦЕНКА СТОЙКОСТИ ФУНКЦИЙ ХЭШИРОВАНИЯ

Аннотация к дипломной работе

Научный руководитель:
ст.н.с. НИИ ППМИ БГУ
кандидат физ.-мат. наук
Пирштук Иван Казимирович

Минск, 2016

РЕФЕРАТ

Дипломная работа, 45 с., 4 рис., 1 табл., 10 источников.

ФУНКЦИЯ ХЭШИРОВАНИЯ, КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННЫХ, АУТЕНТИЧНОСТЬ ДОКУМЕНТА, КОЛЛИЗИЯ ХЭШ-ФУНКЦИИ, ЛАВИННЫЙ ЭФФЕКТ, СЖИМАЮЩАЯ ФУНКЦИЯ.

Объект исследования – функции хэширования. Цель работы – изучение наиболее актуальных подходов контроля целостности данных на основе хэш-функций, выявление их преимуществ и недостатков.

Результатами является рассмотрение актуальных подходов проектирования криптографических функций хэширования, выделение их преимуществ и недостатков, рассмотрение возможных проводимых атак на хэш-функции, реализация некоторых функций хэширования.

Областью применения являются криптографические системы для защиты данных, электронная цифровая подпись, ассоциативные массивы.

SUMMARY

Graduation assignment, 45 p., 4 pic., 1 t., 10 sources.

HASH FUNCTION, CONTROL DATA INTEGRITY, THE AUTHENTICITY OF DOCUMENTS, COLLISION OF HASH FUNCTION, THE AVALANCHE EFFECT, CONTRACTIVE FUNCTION.

Object of study - the hash function. Purpose - to study the most relevant data integrity control approaches based on hash functions, identifying their strengths and weaknesses.

The results is a review of current approaches the design of cryptographic hash functions, highlighting their strengths and weaknesses, consideration of possible carried out attacks on a hash function, the implementation of some hash functions.

Application areas are cryptographic systems for data protection, digital signature and associative arrays.