БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к магистерской диссертации

«Реализация архитектуры криптографических токенов»

Чмырева Мария Александровна

Научный руководитель – кандидат физико-математических наук Агиевич С.В.

Минск, 2020

Реферат

Магистерская диссертация, 37 страница, 18 рисунков, 10 источников.

БЕЗОПАСНОСТЬ, АУТЕНТИФИКАЦИЯ, КРИПТОГРАФИЧЕСКИЕ ТОКЕНЫ, КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ, ДИАГРАММЫ СОСТОЯНИЙ.

Объект исследования **–** криптографический токен.

Цель работы – оценить практическую осуществимость (proof-of-concept) и безопасность архитектуры криптографических токенов *СТБ 34.101.79*.

Методы исследования – построение диаграмм состояний, написание тестов, работа со стандартами Республики Беларусь, построение и реализация архитектуры криптографического токена.

Результат – были построены диаграммы состояний, с их помощью был проанализирован рассмотренный стандарт. Полученные с помощью диаграмм состояний автоматы криптографического токена были протестированы. На основании стандарта и его требований была построена схема и заложена основа для реализации криптографического токена и сопутствующих компонентов на языке *C*.

Область применения – массовая аутентификация с предоставлением идентификационных данных.

Abstract

Master’s thesis, 37 pages, 18 pictures, 10 references.

SECURITY, AUTHENTICATION, CRYPTOGRAPHIC TOKENS, CRYPTOGRAPHIC PROTOCOLS, STATE DIAGRAMS.

Object of research **–** cryptographic token.

Research goal – review feasibility and security of architecture for cryptographic tokens from «*СТБ 34.101.79*». Implement proof-of-concept.

Research methods – creating state diagrams, test writings, work with Belarusian standards, build detailed description and implement cryptographic token architecture.

Result **–** created state diagrams, reviewed standard was analysed with there help. Obtained states were tested. Was created scheme and started implementation for cryptographic token architecture and related components on *C* language based on standard and it's requirements.

Application field – mass authentication with providing of identification data.