МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Чмырева
Мария Александровна

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ПРОТОКОЛОВ ФОРМИРОВАНИЯ ОБЩЕГО КЛЮЧА НА ОСНОВЕ ПАРОЛЕЙ

Аннотация к дипломной работе

Научный руководитель:
Заведующий кафедрой,
кандидат физико-математических наук
И. А. Бодягин

Минск, 2018

Реферат

Отчет по дипломной работе: 27 с., 0 таблиц, 8 рис., 1 приложение, 11 источников

Ключевых слова – протоколы, общий ключ, пароль, Диффи-Хеллман, BPACE.

Объект исследования – протоколы формирования общего ключа.

Цель работы – исследовать протоколы на основе протокола Диффи-Хеллмана и реализовать программу на основе протокола одного из них.

Результаты – был проанализирован протокол BPACE, была написана программа реализующая этот протокол, он также был рассмотрен в контексте клиент/сервер.

Результаты дипломной работы будут включены в официальную библиотеку и использоваться в дальнейшим различными юридическими лицами.

Summary

Report on the degree work: 27 pages, 0 tables, 8 images, 1 attachments, 11 sources.

Keywords: protocols, common key, password, Diffie-Hellman, BPACE.

Research object: password authenticated key agreement.

Aims: do research of protocols based on Diffie-Hellman protocol and implement program based on one of them.

Results: was analyzed BPACE protocol, was wrote program implements it, also it was examined in client/server context.

Results of this work will be included in official library and will be using by different legal persons.