

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

РАЗРАБОТКА КРИПТОСТОЙКОГО СЕТЕВОГО ПРИЛОЖЕНИЯ

Моисеенко Тимофей Алексеевич

Научный руководитель:
кандидат физ.-мат. наук,
доцент Л. Л. Голубева

2022

В дипломной работе 52 страницы, 11 рисунков, 17 источников, 1 приложение из 9 страниц.

КОМПЬЮТЕРНЫЕ СЕТИ, КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ OSI, TCP/IP, СЕТЕВЫЕ ПРОТОКОЛЫ, КРИПТОГРАФИЯ

Объектом исследования дипломной работы являются компьютерные сети и сетевые протоколы.

Целью дипломной работы является создание сетевого протокола для безопасной передачи сообщений по сети, а также создания приложения на основе этого протокола.

Для достижения поставленной цели были использованы: язык программирования Python, модуль для криптографических операций cryptography.

В дипломной работе получены следующие результаты:

1. Описан сетевой протокол прикладного уровня пригодный для передачи данных в IP сетях, гарантирующий конфиденциальность, целостность и аутентичность сообщений.

2. Разработано приложение для нескольких платформ, в том числе и мобильных, позволяющее устройствам обмениваться сообщениями согласно ранее описанному протоколу.

Дипломная работа является завершённой, поставленные задачи решены в полной мере, присутствует возможность дальнейшего развития исследований.

Дипломная работа выполнена автором самостоятельно.

This thesis project is presented in the form of an explanatory note of 52 pages, 11 figures, 17 references, 1 application of 9 pages.

COMPUTER NETWORKS, OSI CONCEPTUAL MODEL, TCP/IP, NETWORK PROTOCOLS, CRYPTOGRAPHY

The research object of this thesis project is to study computer networks and network protocols.

The purpose of this work is to create a network protocol for the secure transmission of messages over a network, and to create an application based on this protocol.

The following methods and tools were used to achieve the goal: Python programming language, cryptography module for cryptography operations.

The main results of the thesis project are as follows:

1. Defined an application layer network protocol suitable for data transmission in IP networks that guarantees confidentiality, integrity and authenticity of messages.
2. An application has been developed for several platforms, including mobile, allowing devices to exchange messages according to the previously described protocol.

The thesis project is complete, all tasks have been successfully done, there is a possibility for further research and development.

The thesis project was done solely by the author.