БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

ЗАЩИТА ИНФОРМАЦИИ В СЕРВИСАХ ИНТЕРНЕТА ВЕЩЕЙ

Гедимин Виталий Валерьевич

Научный руководитель – кандидат технических наук, доцент Мулярчик К.С.

2018

РЕФЕРАТ

Дипломный проект: 50 страниц, 8 иллюстраций, 2 таблиц, 12 источников, 5 приложений.

ЗАЩИТА ИНФОРМАЦИИ В СЕРВИСАХ ИНТЕРНЕТА ВЕЩЕЙ ИНТЕРНЕТ ВЕЩЕЙ, КРИПТОГРАФИЯ, MQTT, ESP32, СИММЕТРИЧНОЕ ШИФРОВАНИЕ, БЛОЧНЫЕ ШИФРЫ, ПОТОЧНЫЕ ШИФРЫ, ГОСТ 28147-89, AES-128, PRESENT, TRIVIUM

Объектом исследования являются способы обеспечения конфиденциальности информации в сервисах интернета вещей с помощью симметричного шифрования.

Цель работы – реализация конфиденциального обмена сообщениями между устройствами сервиса интернета вещей.

Проведен анализ существующих методов и недостатков защиты информации в сервисах интернета вещей. Реализованы наиболее подходящие для устройств сервисов интернета вещей методы симметричного шифрования. Реализован конфиденциальный обмен данными между двумя устройствами сервиса интернета вещей.

РЭФЕРАТ

Дыпломны праект: 50 старонак, 8 ілюстрацый, 2 табліц, 12 крыніц, 5 прыкладанняў.

АБАРОНА ІНФАРМАЦЫІ Ў СЭРВИСЕ ІНТЭРНЭТУ РЭЧАЎ

ІНТЭРНЭТ РЭЧАЎ, КРЫПТАГРАФІЯ, MQTT, ESP32, СІМЕТРЫЧНАЕ ШИФРАВАННЕ, БЛОКАВЫЯ ШЫФРЫ, ПАТОКАВЫЯ ШЫФРЫ, ГОСТ 28147-89, AES-128, PRESENT, TRIVIUM

Аб'ектам даследавання з'яўляюцца спосабы забеспячэння прыватнасці інфармацыі ў сэрвісах інтэрнэту рэчаў з дапамогай сіметрычнага шыфравання.

Мэта работы - рэалізацыя прыватнага абмену паведамленнямі паміж прыладамі сэрвісу інтэрнэту рэчаў.

Праведзены аналіз існуючых метадаў і недахопаў абароны інфармацыі ў сэрвісах інтэрнэту рэчаў. Рэалізаваны найбольш прыдатныя для прылад сэрвісаў інтэрнэту рэчаў метады сіметрычнага шыфравання. Рэалізаваны канфідэнцыйны абмен дадзенымі паміж двума прыладамі сэрвісу інтэрнэту рэчаў.

ABSTRACT

Diploma project: 50 pages, 8 illustrations, 2 tables, 12 sources, 5 applications.

PROTECTION OF INFORMATION IN SERVICE OF THE INTERNET OF THINGS

INTERNET OF THINGS, CRYPTOGRAPHY, MQTT, ESP32, SYMMETRIC ENCRYPTION, BLOCK CIRCUITS, STREAMS, GOST 28147-89, AES-128, PRESENT, TRIVIUM

The subject of the study are ways to ensure the confidentiality of information in the Internet of things using symmetric encryption.

The goal of the work is the implementation of confidential messaging between devices of the Internet service of things.

The analysis of existing methods and deficiencies of information security in Internet services of things is carried out. The methods of symmetric encryption most suitable for devices of Internet services of things are implemented. The confidential data exchange between two devices of the Internet of things service is realized.