НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра програмного забезпечення комп'ютерних систем

«До захисту допущено»
Науковий керівник кафедри
_____ І.А. Дичка
(підпис)
"___" _____ 2017 р.

Дипломний проект

на здобуття ступеня бакалавра
з напряму підготовки 6.050103 "Програмна інженерія"

на тему СЕРВІС КОРИСТУВАЦЬКИХ ОПОВІЩЕНЬ ДЛЯ ОДНОРАНГОВОЇ МЕРЕЖІ ЕЛЕКТРОННОЇ ТОРГІВЛІ OPENBAZAAR

Виконав: студент 4 курсу, групи КП-32
Жикін Юрій Сергійович _____ (підпис)

Керівник доц., доц., к.т.н. Марченко О.І. _____ (підпис)

Консультант з нормоконтролю старший викладач Онай М.В. _____ (підпис)

Рецензент зав. відділом, с.н.с., к.т.н. Андрієнко А.А. _____ (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2017

АНОТАЦІЯ

Даний дипломний проект присвячений створенню сервісу псевдонімних користувацьких оповіщень для однорангової мережі електронної торгівлі OpenBazaar.

Сервіс представляє собою web-додаток, що дозволяє власнику магазину в мережі OpenBazaar неінтерактивно створювати одноразові ключі, за якими його потенційні клієнти можуть одноразово здійснити оповіщення у випадку необхідності термінового зв’язку. Для цього клієнту надається простий прикладний програмний інтерфейс з трьох функцій: 1) реєстрація — розміщення своїх контактних даних в сховищі сервісу; 2) верифікація — допоміжна функція підтвердження контактних даних при здійсненні реєстрації; 3) пересилання повідомлення — функція передачі повідомлення за умови наявності в клієнта спеціального одноразового ключа. При цьому описано і розроблено спеціальний криптографічний протокол генерації та верифікації одноразових ключів для делегованої автентифікації.

У даному дипломному проекті розроблено архітектуру та прикладний програмний інтерфейс сервісу, а також два криптографічні протоколи генерації/верифікації одноразових ключів для делегованої автентифікації (тестовий на основі модифікації протоколу ланцюгів Лампорта та основний на основі протоколу CryptoNote).

ABSTRACT

This diploma project deals with the development of pseudonymous user notification service for OpenBazaar e-commerce peer-to-peer network.

The service is a web-application that allows OpenBazaar network store owners to non-interactively create one-time keys, which can be used by their potential clients to send one-time notification in case emergency communication is required. For this purpose, service provides a simple API, that consists of three functions: 1) registration — process of adding personal contact data to the service's data store; 2) verification — supplementary function that allows to confirm access to the contact accounts during the registration phase; 3) forwarding — function that allows to pass the message from sender to the receiver in case sender provides correct one-time key. During the course of work, special cryptographic protocol was designed, that allows for generating and verifying one-time keys for delegated authentication.

The following structures and algorithms are developed in this project: the architecture and API of the service, as well as two cryptographic protocols for generation/verification of one-time keys for delegated authentication (test protocol based on Lamport's scheme and main protocol based on CryptoNote cryptocurrency protocol).