БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ЭЦП С ИСПОЛЬЗОВАНИЕМ ПАК «ПОДПИСЬ»

Лопорт Александр Викторович

Научный руководитель – кандидат технических наук,

старший преподаватель Труханович А. Л.

2020

РЕФЕРАТ

Дипломная работа 63 страниц, 19 рисунков (схемы, скриншоты), 6 таблиц, 6 источников.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ; КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ; ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «ПОДПИСЬ»; ИНТЕРФЕЙС,

Объект исследования – программно-аппаратный комплекс «Подпись». В работе было исследовано назначение и функциональные возможности ПАК «Подпись», библиотека bitSignCryptLib, а также алгоритмы шифрования ГОСТ 28147-89 и СТБ П 34.101.31-2007.

Цель работы - разработка интерфейса программы, предоставляющей доступ к функциям ПАК «Подпись».

В работе представлено назначение, функциональные возможности и технические характеристики ПАК «Подпись»; описана библиотека bitSignCryptLib, предоставляющая разработчикам интерфейс прикладного программирования криптографических функций ПАК «Подпись»; описаны алгоритмы шифрования ГОСТ 28147-89 и СТБ П 34.101.31-2007 и режимы их работы; приведены структурные схемы и скриншоты интерфейса программы для ПАК «Подпись». Интерфейс был разработан с использованием технологии .Net Framework 4.7.2 и языка разметки XAML.

РЭФЕРАТ

Дыпломная праца 63 старонак, 19 малюнкаў (схемы, скрыншоты), 6 табліц, 6 крыніц.

ЭЛЕКТРОННЫ ЛІЧБАВЫ ПОДПІС; КРЫПТАГРАФІЧНЫЯ АЛГАРЫТМЫ; ПРАГРАМНА-АПАРАТНЫ КОМПЛЕКС «ПОДПИСЬ»; ІНТЭРФЕЙС.

Аб'ект даследавання - праграмна-апаратны комплекс «Подпись». У рабоце было даследавана прызначэнне і функцыянальныя магчымасці ПАК «Подпись», бібліятэка bitSignCryptLib, а таксама алгарытмы шыфравання ДАСТ 28147-89 і СТБ П 34.101.31-2007 і рэжымы іх працы.

Мэта работы - распрацоўка інтэрфейсу праграмы, якая прадстаўляе доступ да функцый ПАК «Подпись».

У працы прадстаўлена прызначэнне, функцыянальныя магчымасці і тэхнічныя характарыстыкі ПАК «Подпись»; апісана бібліятэка bitSignCryptLib, якая прадстаўляе распрацоўнікам інтэрфейс прыкладнога праграмавання крыптаграфічных функцый ПАК «Подпись»; апісаны алгарытмы шыфравання ДАСТ 28147-89 і СТБ П 34.101.31-2007 і рэжымы іх працы; прыведзены структурныя схемы і скрыншоты інтэрфейсу праграмы для ПАК «Подпись». Інтэрфейс быў распрацаваны з выкарыстаннем тэхналогіі .Net Framework 4.7.2 і мовы разметкі XAML.

ABSTRACT

The degree work 63 pages, 19 figures (schemes, screenshots), 6 tables, 6 sources.

ELECTRONIC DIGITAL SIGNATURE; CRYPTOGRAPHIC ALGORITHMS; SOFTWARE AND HARDWARE COMPLEX «ПОДПИСЬ»; INTERFACE,

The object of the work is the hardware-software complex “Подпись”. In the work, the purpose and functionality of the Signature PAC, the bitSignCryptLib library, as well as the encryption algorithms GOST 28147-89 and STB P 34.101.31-2007, were investigated.

The purpose of the research is to develop an interface for a program that provides access to the functions of the hardware-software complex “Подпись”.

The work presents the purpose, functionality and technical characteristics of the hardware-software complex "Подпись"; The bitSignCryptLib library is described, which provides developers with an interface for application programming of cryptographic functions of the hardware-software complex "Подпись" encryption algorithms are described GOST 28147-89 and STB P 34.101.31-2007 and their modes of operation; structural diagrams and screenshots of the program interface for the hardware-software complex "Подпись" are shown. The interface was developed using .Net Framework 4.7.2 technology and the XAML markup language.