**Министерство образования и науки Российской Федерации**

Федеральное государственное автономное образовательное учреждение   
высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий - РТФ

Департамент радиоэлектроники и связи

**Методические указания к программному продукту** **«Шифратор/Дешифратор»**

Зайков Александр

Зыков Никита

Мухаматнуров Владислав

Павлухин Дмитрий

Екатеринбург 2018

**Аннотация**

Документ представляет собой методические указания к программному продукту «Шифратор/Дешифратор», включающие в себя:

* Определение проблемы, решаемой программным продуктом;
* Определение специфических функциональных требований к программному продукту; определение специфических нефункциональных требований к программному продукту;
* Определение требований к архитектуре программного продукта;
* Описание используемой библиотеки КриптоПро CSP;
* Описание реализации программного продукта;
* Руководство пользователя программного продукта.

**Содержание**

**Содержание**

[**Определение проблемы, решаемой программным продуктом** 4](#_Toc513473978)

[**Определение требований к программному продукту** 5](#_Toc513473979)

[**Определение требований к архитектуре программного продукта** 6](#_Toc513473980)

[**Описание библиотеки КриптоПро CSP** 7](#_Toc513473981)

[**Описание реализации программного продукта** 9](#_Toc513473982)

[**Руководство пользователя программного продукта** 10](#_Toc513473983)

# **1. Определение проблемы, решаемой программным продуктом**

Требуется разработать программу, которая использовалась бы для шифрования файлов и работы с ключевой информацией с использованием алгоритмов ГОСТ. В том числе необходимо предусмотреть её расширение, которое предусматривало бы механизмы асимметричного шифрования и установки соединения VPN.

# **2. Определение требований к программному продукту**

**Специфические функциональные требования:**

1. Программа должна осуществлять создание ключей симметричного шифрования с использованием алгоритмов ГОСТ 3уцорагу
2. Программа должна уметь сохранять создаваемые ключи шифрования.
3. Программа должна уметь шифровать файлы размером до 50Мб с использованием алгоритмов ГОСТ рафругра.
4. Шифрованный файл должен сохраняться в ту же директорию, где находится оригинальный файл
5. Программа должна осуществлять расшифровку файлов с использованием имеющихся ключей шифрования

**Специфические нефункциональные требования:**

1. Программа должна функционировать в операционных системах семейства Windows (XP и выше)
2. Программа должна использовать библиотеку КриптоПро CSP
3. Программа должна обеспечивать полную функциональность при (512 МБ RAM, 2ГГц CPU, 80Гб HDD)

# **3. Определение требований к архитектуре программного продукта**

Требуется разработать программу, которая бы удовлетворяла следующим требованиям:

1. Исходный код программы должен быть написан на языке C++
2. Программа должна состоять из следующих основных частей:

# **4. Описание библиотеки КриптоПро CSP**

Основными функциями КриптоПро CSP являются:

* генерация ключей подписи (256 бит и 512 бит), ключей обмена (256 бит и 512 бит), ключей шифрования (256 бит),
* формирование ключей проверки подписи (512 бит для ГОСТ Р 34.10-2012 с длиной ключа подписи 256 бит (ГОСТ Р 34.10-2001) и 1024 бита для ГОСТ Р 34.10-2012 с длиной ключа подписи 512 бит);
* формирование закрытых ключей на следующие типы носителей:
  + дискета 3,5";
  + процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателей смарт-карт, поддерживающие протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126);
  + индикаторы Touch-Memory DS1993 - DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь", устройство чтения индикаторов Touch-Memory DALLAS;
  + электронный ключ с интерфейсом USB;
  + сменный носитель с интерфейсом USB;
  + реестр Windows, локальный диск ОС UNIX.
* возможность хранения сертификатов открытых ключей в ключевом контейнере;
* возможность генерации ключей с различными параметрами в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 ("*Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.*");
* хэширование данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 ("*Информационная технология. Криптографическая защита информации. Функция хэширования.*");
* шифрование данных во всех режимах, определенных ГОСТ 28147-89 ("*Системы обработки информации. Защита криптографическая.*");
* имитозащита данных в соответствии с ГОСТ 28147-89;
* формирование электронной цифровой подписи в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;
* поддержка функций, режимов, параметров, определённых в RFC 4357;
* опциональное использование пароля (пин-кода) для дополнительной защиты ключевой информации;
* реализация мер защиты от НСД ключевой информации пользователя.

Библиотека КриптоПро CSP позволяет выполнять действия, которые должны быть выполнены КриптоПро CSP путем вызова соответствующих функций. При этом разрабатываемая программа будет представлять собой «оболочку» из которой функции будут вызываться.

Встраивание будет произведено на уровне прикладного программного обеспечения, с использованием интерфейса CryptoApi 2.0. Таким образом будет произведена изоляция прикладного программного обеспечения от крипрографических функций. При этом выбор криптографических алгоритмов будет определяться на уровне программного обесечения.

В соответствии с установленными требованиями в реализации будут использованы следующие функции библиотеки:

* рорлро

# **5. Описание реализации программного продукта**

Приведенные ниже примеры демонстрируют использование основных функций криптопровайдера.

Для уменьшения размера кода примеров следующие 4 строки в них не приводятся:

#include <stdio.h>

#include <windows.h>

#include <wincrypt.h>

#include <wincryptex.h>

Во всех примерах используется функция HandleError для обработки кода ошибок, вывода сообщения и выхода из программы. В приложениях рекомендуется заменить данную функцию другой, которая позволит произвести более подробную диагностику кода ошибки.

# **6. Руководство пользователя программного продукта**