**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ   
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

Департамент программной инженерии

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Доцент департамента программной инженерии факультета компьютерных наук, канд. физ.-мат. наук.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А.Набебин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2015 г. | УТВЕРЖДАЮ  Академический руководитель образовательной программы «Программная инженерия»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2015 г. |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 51 01-1-ЛУ | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  **Программа и методика испытаний**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.501430-01 51 01-1-ЛУ**  Исполнитель  студент группы 102 ПИ  \_\_\_\_\_\_\_\_\_\_\_/Берюхов А.С./  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2015 г.  **2015** | | |  |

УТВЕРЖДЕНО

RU.17701729.501430-01 51 01-1-ЛУ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 51 01-1 | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  Программа и методика испытаний  RU.17701729.501430-01 51 01-1  **Листов 15**  **2015** |  |

**СОДЕРЖАНИЕ**

[1. Объект испытаний 3](#_Toc419631992)

[1.1. Наименование испытуемой программы 3](#_Toc419631993)

[1.2. Область применения испытуемой программы 3](#_Toc419631994)

[1.3. Обозначение испытуемой программы 3](#_Toc419631995)

[2. Цель испытаний 4](#_Toc419631996)

[3. Требования к программе 5](#_Toc419631997)

[3.1. Требования к функциональным характеристикам 5](#_Toc419631998)

[3.1.1. Требования к составу выполняемых функций 5](#_Toc419631999)

[3.1.2. Требования к организации входных данных 5](#_Toc419632000)

[3.1.3. Требования к организации выходных данных 5](#_Toc419632001)

[3.2. Требования к интерфейсу 5](#_Toc419632002)

[3.3. Требование к надежности 6](#_Toc419632003)

[3.4. Требования к информационной и программной совместимости 6](#_Toc419632004)

[3.4.1. Требования к исходному коду 6](#_Toc419632005)

[3.4.2. Требования к программным средствам, используемым программой 6](#_Toc419632006)

[3.4.3. Требования к защите информации и программы 7](#_Toc419632007)

[3.5. Требования к маркировке и упаковке 7](#_Toc419632008)

[4. Требования к программной документации 8](#_Toc419632009)

[4.1. Состав программной документации 8](#_Toc419632010)

[4.2. Специальные требования к программной документации 8](#_Toc419632011)

[5. Средства и порядок испытаний 9](#_Toc419632012)

[5.1. Технически средства, используемые во время испытаний 9](#_Toc419632013)

[5.2. Программные средства, используемые во время испытаний 9](#_Toc419632014)

[5.3. Порядок проведения испытаний 9](#_Toc419632015)

[6. Методы испытаний 10](#_Toc419632016)

[6.1. Проверка требований к функциональным характеристикам 10](#_Toc419632017)

[6.2. Проверка требований к интерфейсу 10](#_Toc419632018)

[6.3. Проверка требований к надежности 12](#_Toc419632019)

[6.4. Проверка требований к информационной и программной совместимости 13](#_Toc419632020)

[6.5. Проверка требований к маркировке и упаковке 13](#_Toc419632021)

[6.6. Проверка требований к программной документации 13](#_Toc419632022)

[7. Приложения 14](#_Toc419632023)

[7.1. Список используемой литературы 14](#_Toc419632024)

# 1. Объект испытаний

## 1.1. Наименование испытуемой программы

Наименование программы – «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи».

## 1.2. Область применения испытуемой программы

«Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи» – программа, реализующая шифрование цифровых данных с помощью алгоритма А5-1.

Задача программы заключается в обеспечении возможности обратимого преобразования информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. [1]

Решение данной задачи имеет потенциальное приложение в разных областях:

1. Передача голосовых данных по каналам мобильной связи – обеспечение конфиденциальности передаваемых данных между абонентом и базовой станцией.
2. Передача информации от адресанта к адресату без возможности доступа к ней третьими лицами.
3. Хранение информации в зашифрованном виде.

## 1.3. Обозначение испытуемой программы

Обозначение для программы – А5КоДек.

# 2. Цель испытаний

Цель проведения испытаний программного продукта – проверка соответствия характеристик продукта предъявленным требованиям, обозначенных в документе Техническое задание.

# 3. Требования к программе

## 3.1. Требования к функциональным характеристикам

### 3.1.1. Требования к составу выполняемых функций

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

1. Выбор файла для шифрования / дешифрования.
2. Выбор файла, в который будет записан результат работы программы.
3. Ввод ключа.
4. Получение результата в виде шифрованного / дешифрованного файла в указанном пользователем директории под указанным именем.

### 3.1.2. Требования к организации входных данных

Программа должна предоставлять возможность открытия файла любого формата (с любым расширением), любого размера.

### 3.1.3. Требования к организации выходных данных

Программа должна предоставлять возможность сохранения шифрованного/дешифрованного файла с любым.

## 3.2. Требования к интерфейсу

Интерфейс программного продукта должен представлять собой Windows-интерфейс.

В программе должно быть спроектировано окно, которое открывается при запуске программы и обеспечивает процесс шифрования / дешифрования.

В этом окне должны присутствовать:

1. Кнопка, вызывающая диалоговое окно выбора файла для открытия.
2. Кнопка, вызывающая диалоговое окно выбора файла для сохранения.
3. Текстовое поле и кнопку, предназначенные для ввода ключа.
4. Индикатор выполнения процесса шифрования.

Программа должна иметь русскоязычный интерфейс.

Программа должна иметь справку для пользователя.

Установка программы должна осуществляться из одного exe-файла с помощью инсталлятора.

## 3.3. Требование к надежности

Для устойчивой работы программного продукта необходима устойчивая работа технического устройства, на котором запускается продукт, а также программных компонентов на нем.

Программа должна обрабатывать все исключительные ситуации, такие как:

* Ошибка чтения входного файла.
* Ошибка записи в выходной файл.
* Неверный формат ключа.

## 3.4. Требования к информационной и программной совместимости

### 3.4.1. Требования к исходному коду

1. программа должна быть реализована на языке C# 4.0;
2. среда программирования – Microsoft Visual Studio 2010 или 2012;
3. при разработке программы должна быть использована платформа .NET Framework версии не старше 2.0.

### 3.4.2. Требования к программным средствам, используемым программой

1. операционная система Microsoft Windows XP и новее;
2. установленный Microsoft .NET Framework 2.0.

### 3.4.3. Требования к защите информации и программы

Требования к защите программы и информации не предъявляются.

## 3.5. Требования к маркировке и упаковке

Приложение распространяется на компакт диске (CD), флэш носителе или посредством сети Интернет. Диск должен быть обязательно подписан "Курсовая работа, ФИО, группа, 2015". В корне флэш носителя должен быть файл readme.txt с указанием этой информации. Для работы программы требуется инсталляция.

# 4. Требования к программной документации

## 4.1. Состав программной документации

В процессе разработки должны быть созданы следующие документы:

1) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Техническое задание (ГОСТ 19.201-78);

2) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Текст программы (ГОСТ 19.401-78);

3) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Пояснительная записка (ГОСТ 19.404-79);

4) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Программа и методика испытаний (ГОСТ 19.301-78);

5) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Руководство оператора (ГОСТ 19.505-79);

5) «Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи». Руководство программиста (ГОСТ 19.504-79).

## 4.2. Специальные требования к программной документации

1) Вся документация должна быть составлена согласно ЕСПД (ГОСТ 19.101-77, 19.104-78, 19.105-78, 19.106-78 и ГОСТ к соответствующим документам (см. выше)) [2].

2) Вся документация сдаётся в печатном виде, с подписанными листами утверждения.

3) Вся документация сдаётся в электронном виде в составе курсовой работы в систему LMS НИУ ВШЭ.

# 5. Средства и порядок испытаний

## 5.1. Технически средства, используемые во время испытаний

Компьютер, со следующими свойствами:

1. Процессор Pentium с частотой 233 МГц или более быстрый (рекомендуется не менее 300 МГц).
2. Не менее 64 МБ оперативной памяти (рекомендуется не менее 128 МБ).
3. Не менее 1,5 ГБ свободного места на жестком диске.
4. Дисковод для компакт- или DVD-дисков.
5. Клавиатура, мышь Microsoft Mouse или совместимое указывающее устройство.
6. Видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек.

## 5.2. Программные средства, используемые во время испытаний

1. операционная система Microsoft Windows XP и новее;
2. установленный Microsoft .NET Framework 2.0.

## 5.3. Порядок проведения испытаний

1. Проверка требований к функциональным характеристикам.
2. Проверка требований к интерфейсу.
3. Проверка требований к надежности.
4. Проверка требований к информационной и программной совместимости.
5. Проверка требований к маркировке и упаковке.
6. Проверка требований к программной документации.

# 6. Методы испытаний

Для проведения первых четырех пунктов испытаний (см. п.5.3) необходимо установить приложение на компьютер (см. Руководство оператора, п.3.1).

## 6.1. Проверка требований к функциональным характеристикам

Для проверки требований к функциональным характеристикам, запускаем программу и пробуем зашифровать любой тестовый файл.

Заметим, что программа обеспечивает, как и требовалось, возможность выбора файла для шифрования, файла, в который будет записан результат работы программы, требует ввода ключа и сохраняет результат шифрования в указанном каталоге под указанным именем.

Кроме того, при двукратно применении программы, файл результата совпадает с первоначальным тестовым файлом. Значит, программа соответствует заявленным функциональным требованиям.

## 6.2. Проверка требований к интерфейсу

Необходимо проверить выполнение всех обозначенных требований к интерфейсу.

Интерфейс программного продукта представляет собой Windows-интерфейс.

В программе спроектировано окно, которое открывается при запуске программы и обеспечивает процесс шифрования / дешифрования.

В этом окне присутствуют (рис.1 и 2):

1. Кнопка, вызывающая диалоговое окно выбора файла для открытия.
2. Кнопка, вызывающая диалоговое окно выбора файла для сохранения.
3. Текстовое поле и кнопку, предназначенные для ввода ключа.
4. Индикатор выполнения процесса шифрования.

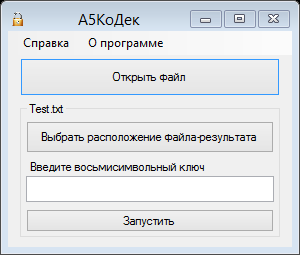


Рисунок 1

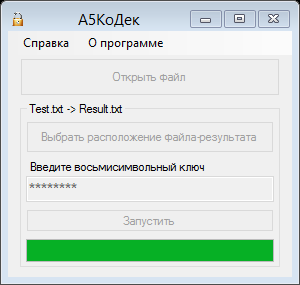
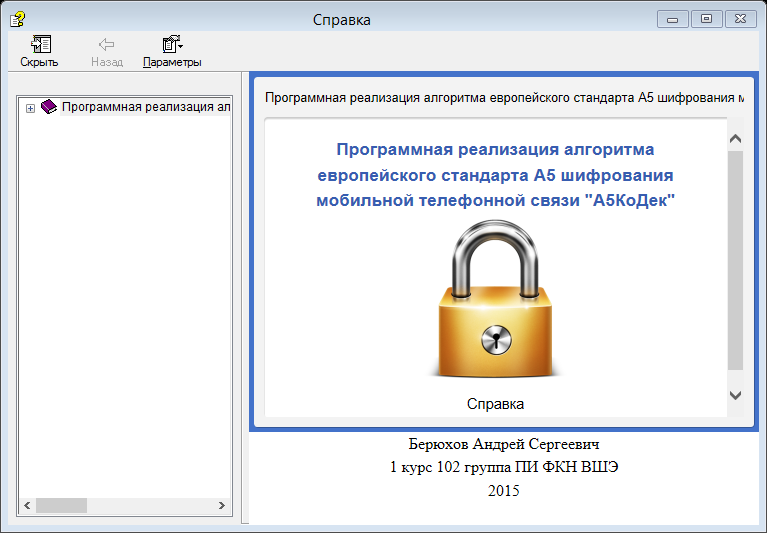


Рисунок 2

Программа имеет русскоязычный интерфейс.

Программа имеет справку для пользователя (рис.3).



Рисунок

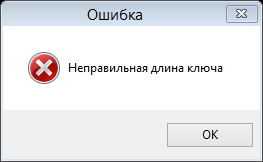
Установка программы осуществляется из одного exe-файла с помощью инсталлятора.

Интерфейс программы соответствует заявленным требованиям.

## 6.3. Проверка требований к надежности

Для проверки выполнения требований к надежности, необходимо спровоцировать (если возможно) появление исключительных ситуаций.

Как и требовалось, при неверно формате ключа возникает ошибка «Неправильная длина ключа» (рис.4). При этом программа продолжает свою работу.



Рисунок

В ходе тестирования программа не создавала других необработанных исключительных ситуаций. Требования к надежности соблюдены.

## 6.4. Проверка требований к информационной и программной совместимости

Программа реализована на языке C# 4.0 с использованием платформы .NET Framework 2.0 в среде Microsoft Visual Studio 2012. Приложение работает на ОС Microsoft Windows XP и новее. Предъявленные требования соблюдены.

## 6.5. Проверка требований к маркировке и упаковке

Проверка осуществляется визуально.

Приложение распространяется на компакт диске (CD), диск подписан "Курсовая работа, ФИО, группа, 2015". Для работы программы требуется инсталляция. Требования к маркировке и упаковке соблюдены.

## 6.6. Проверка требований к программной документации

Проверка программной документации начинается с проверки наличия всех обозначенных документов в печатном виде и подписей на их листах утверждения, а также проверки наличия электронных версий в системе LMS НИУ ВШЭ. После этого необходимо проверить соответствие документов ЕСПД (ГОСТ).

Все представленные документы соответствуют обозначенным требованиям.

# 7. Приложения

## 7.1. Список используемой литературы

1. Шифрование. Материал из Википедии — свободной энциклопедии [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/Шифрование> (Дата обращения 14.02.2015, режим доступа: свободный).

2. Единая система программной документации – М.: ИПК Издательство стандартов, 2000.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в документе | № документа | Входящий № сопроводительного документа и дата | Подпись | Дата |
| измененных | замененных | новых | аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |