**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 34 01-1-ЛУ | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  **Руководство оператора**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.501430-01 34 01-1-ЛУ**  Исполнитель  студент группы 102 ПИ  \_\_\_\_\_\_\_\_\_\_\_/Берюхов А.С./  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2015 г.  **2015** | | |  |

УТВЕРЖДЕНО

RU.17701729.501430-01 34 01-1-ЛУ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 34 01-1 | | **Программная реализация алгоритма европейского стандарта А5 шифрования мобильной телефонной связи**  Руководство оператора  RU.17701729.501430-01 34 01-1  **Листов 17**  **2015** |  |

**АННОТАЦИЯ**

Документ «Руководство оператора» адресован пользователям данного программного продукта и предназначен для облегчения процесса ознакомления и использования с приложением.

Руководство операторасодержит четыре основных части: Назначение программы, Условия выполнения программы, Выполнение программы и Сообщения оператору.

В разделе Назначение программы описаны функциональное и эксплуатационное назначение данной программы, а также состав выполняемых функций.

В разделе Условия выполнения программы указаны минимальные технические и программные требования, необходимые для установки и запуска программы, а также минимальные требования к пользователю.

В разделе Выполнение программы приведена пошаговая инструкция по установке и эксплуатации данного программного продукта.

В разделе Сообщения оператору перечислены основные сообщения (ошибки), которые могут возникнуть в процессе работы программы и указаны действия по их устранению.

**СОДЕРЖАНИЕ**

[1. Назначение программы 4](#_Toc419708216)

[1.1. Функциональное назначение 4](#_Toc419708217)

[1.2. Эксплуатационное назначение 4](#_Toc419708218)

[1.3. Состав функций 4](#_Toc419708219)

[2. Условия выполнения программы 5](#_Toc419708220)

[2.1. Минимальный состав аппаратных средств 5](#_Toc419708221)

[2.2. Минимальный состав программных средств 5](#_Toc419708222)

[2.3. Требования к пользователю 5](#_Toc419708223)

[3. Выполнение программы 6](#_Toc419708224)

[3.1. Установка и запуск программы 6](#_Toc419708225)

[3.2. Работа программы 10](#_Toc419708226)

[3.2.1. Основные функции 10](#_Toc419708227)

[3.2.2. Справка 13](#_Toc419708228)

[3.2.3. О программе 14](#_Toc419708229)

[4.Сообщения оператору 15](#_Toc419708230)

[5. Приложения 16](#_Toc419708231)

[5.1. Список используемой литературы 16](#_Toc419708232)

# 1. Назначение программы

## 1.1. Функциональное назначение

Программа предназначена для осуществления потокового шифрования и дешифрования любых файлов, представленных в двоичном виде; реализованного алгоритмом А5-1, схожим с используемым для шифрования мобильной связи. Программа должна скрывать информацию от неавторизованных лиц (не имеющих аутентичного ключа) и давать доступ к ней авторизованным (имеющим ключ).

## 1.2. Эксплуатационное назначение

Программа предназначена для защиты информации от несанкционированного использования. Она позволяет решать проблемы создания защищенного канала связи и хранения информации в виде, недоступном третьим (неавторизованным) лицам.

## 1.3. Состав функций

Программа выполняет следующие функции:

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.

# 2. Условия выполнения программы

## 2.1. Минимальный состав аппаратных средств

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. [1]

## 2.2. Минимальный состав программных средств

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

## 2.3. Требования к пользователю

Программа не требует специальных знаний и специального обслуживания. Требуемая квалификация пользователя – оператор ЭВМ, обладающий навыками использования графического интерфейса операционной системы Windows.

# 3. Выполнение программы

В этом параграфе будут описаны и проиллюстрированы основные моменты работы приложения.

## 3.1. Установка и запуск программы

Приложение может распространяться на компакт диске (CD), флэш носителе или посредством сети Интернет. В комплекте поставки содержится приложение в виде исполняемого файла и могут входить техническая документация и презентация проекта.

Для установки программы необходимо запустить файл с названием A5CoDecSetup.exe. После запуска появится окно (рис.1).

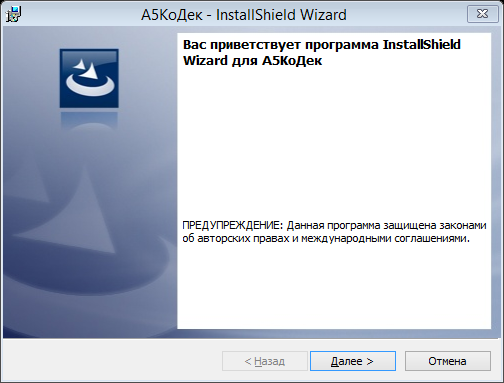


Рисунок 1

После ознакомления с информацией, представленной в данном окне, необходимо нажать кнопку «Далее >». Появится окно «Папка назначения» (рис.2).

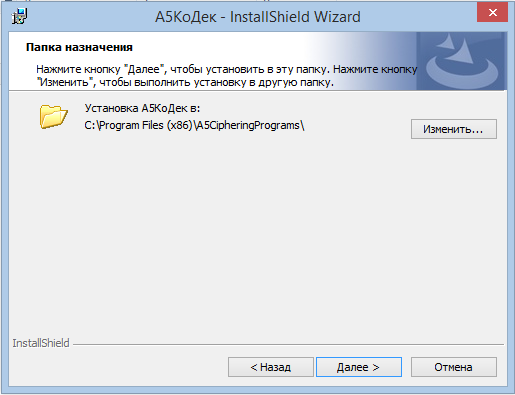


Рисунок 2

Если необходимо, измените каталог для установки, нажав на кнопку «Изменить…». Затем нажмите кнопку «Далее >». Появится следующее окно «Готова к установке программы» (рис.3).

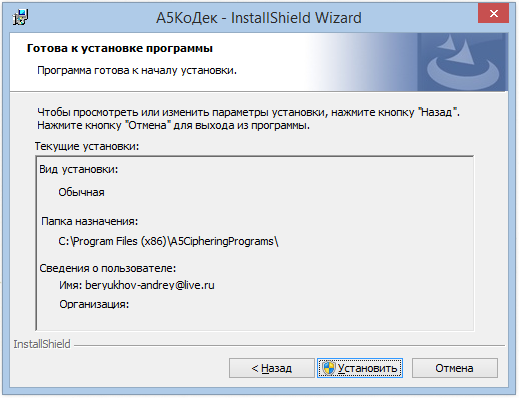


Рисунок 3

Ознакомьтесь с параметрами установки. Если всё верно, нажмите «Установить», иначе «< Назад» и измените параметры.

Если вы нажали «Установить», последовательно возникнут два окна: «Установка А5КоДек» (рис. 4) и «Программа InstallShield Wizard завершена» (рис. 5).

В последнем выберите галочку «Запустить программу», если хотите запустить программу, и нажмите кнопку «Готово».

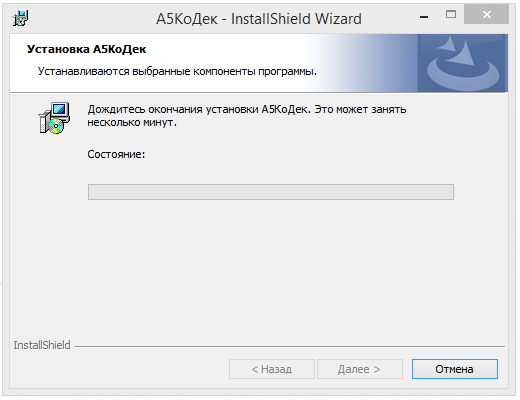


Рисунок 4

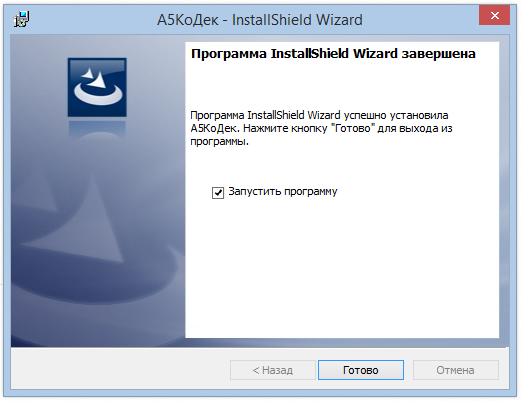


Рисунок 5

После установки на рабочем столе появится ярлык «Launch A5CoDec.exe» (рис. 6).



Рисунок 6

Для запуска программы кликните два раза по этому ярлыку.

## 3.2. Работа программы

После запуска программы отобразится основное окно (рис. 7).

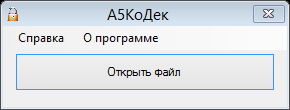


Рисунок 7

### 3.2.1. Основные функции

Для того, чтобы начать шифрование или дешифрование (процедура одинакова, поэтому в дальнейшем будем говорить только о шифровании) нажмите кнопку «Открыть файл». Откроется диалоговое окно выбора файла для шифрования (рис.8).

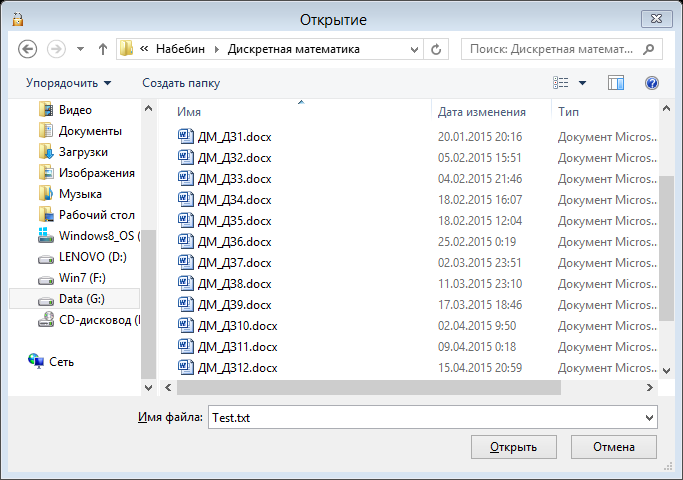


Рисунок 8

Выберите файл и нажмите кнопку «Открыть». Диалоговое окно закроется, а главное окно поменяет свой вид (рис.9).

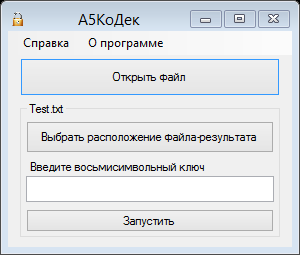


Рисунок 9

Далее нажмите кнопку «Выбрать расположение файла-результата». Откроется диалоговое окно Сохранение (рис.10), в котором Вам необходимо выбрать существующий файл, или выбрать каталог и ввести имя нового файла, например, Result.txt. Рекомендуется сохранять файл с тем же расширением, что и исходный.

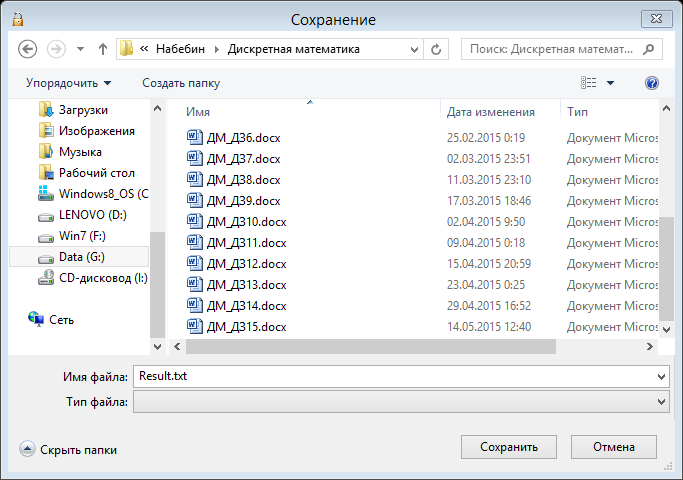


Рисунок 10

Затем нажмите кнопку «Сохранить». Диалоговое окно закроется. В главном окне (рис. 9) в поле «Введите восьмисимвольный ключ» введите восемь символов ключа. Затем нажмите кнопку «Запустить». В процессе шифрования в окне появится строка состояния (рис.11). По окончании отобразится окно с заголовком Успех и сообщением о завершении создания зашифрованного (или расшифрованного) файла.

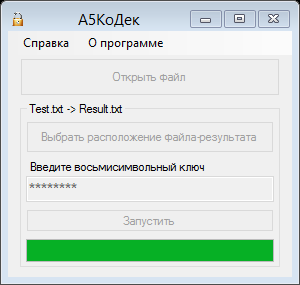


Рисунок 11

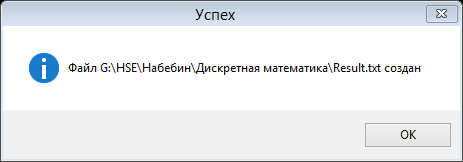


Рисунок 12

### 3.2.2. Справка

При нажатии на кнопку «Справка» (рис.7) откроется файл справки(рис.13).

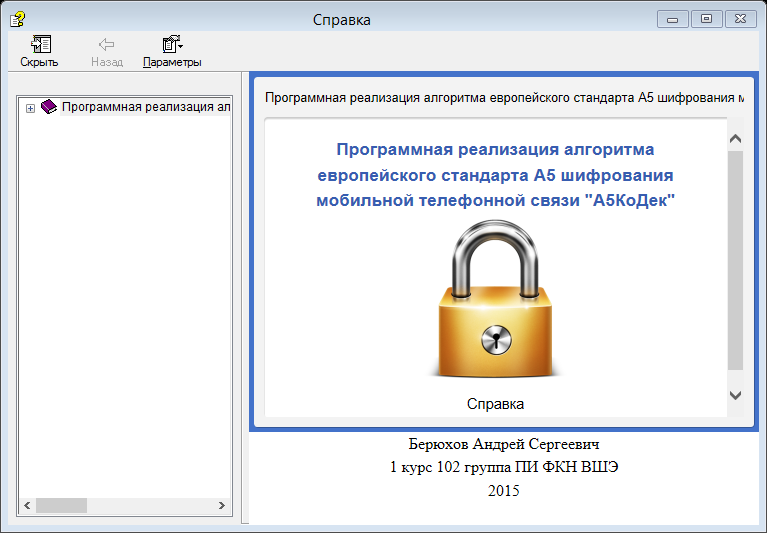


Рисунок 13

На её страницах отображена основная информации о пользовании программой. Нажмите кнопку «Х» в правом верхнем углу для её закрытия.

### 3.2.3. О программе

При нажатии на кнопку «О программе» (рис.7) откроется окно с данными об авторе программы (рис.14).

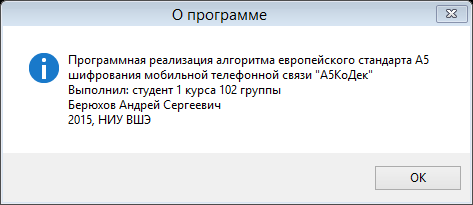
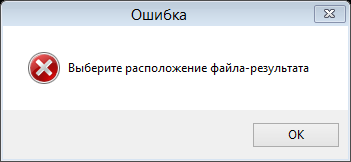


Рисунок 14

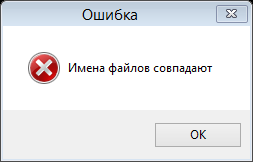
# 4.Сообщения оператору

1. Ошибка «Выберите расположение файла-результата» (рис.15). Возникает при нажатии на кнопку «Запустить» без предварительного выбора файла для сохранения результата шифрования. Для закрытия окна необходимо нажать «ОК» или «Х» в правом верхнем углу окна.



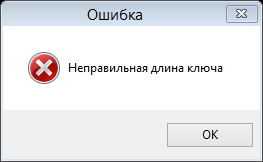
Рисунок

2. Ошибка «Имена файлов совпадают» (рис.16). Возникает при выборе в качестве файла для шифрования и файла для результата одного и того же файла. Для закрытия окна необходимо нажать «ОК» или «Х» в правом верхнем углу окна.



Рисунок

3. Ошибка «Неправильная длина ключа» (рис.17). Возникает при пустом поле для ввода ключа или длине введенного ключа, отличном от восьми символов. Для закрытия окна необходимо нажать «ОК» или «Х» в правом верхнем углу окна.



Рисунок

# 5. Приложения

## 5.1. Список используемой литературы

1. Системные требования для операционных систем Windows ХР [Электронный ресурс] / URL: <https://support.microsoft.com/ru-ru/kb/314865> (Дата обращения 20.02.2015, режим доступа: свободный).

2. Единая система программной документации – М.: ИПК Издательство стандартов, 2000 (ГОСТ 19.505-79).

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