

**МИНОБРНАУКИ РОССИИ**

**федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Московский государственный технологический университет «СТАНКИН»**

**(ФГБОУ ВО «МГТУ «СТАНКИН»)**

|  |  |
| --- | --- |
| **ИНСТИТУТ**  информационных систем  и технологий | **Кафедра**  информационных систем |

**КУРСОВОЙ ПРОЕКТ**

по дисциплине «**Проектирование информационных систем**»

на тему: Проектирование системы шифрования.

Направление **09.03.02 Информационные системы и технологии**

|  |  |
| --- | --- |
| Студент  группы ИДБ-15-12 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Марков А.А.**  подпись |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Овчинников П.Е.**  подпись |

Оглавление

[Введение 3](#_Toc532502543)

[Глава 1. Функциональная модель (IDEF0) 4](#_Toc532502544)

[Глава 2. Модель потоков данных (DFD) 8](#_Toc532502545)

[Глава 3. Диаграммы классов (ERD) 9](#_Toc532502546)

[Заключение 10](#_Toc532502547)

# Введение

Система шифрования предназначена для шифрования данных пользователя и отправки их на сервер.

Программное обеспечение системы состоит из системы шифрования данных и предназначено для решения следующих задач:

1. Определения типа входных данных;
2. Шифрования данных ассиметричным алгоритмом шифрования;
3. Отправка зашифрованных данных на сервер.

Объектом исследования является процесс верификации.

Исследования выполняются путем построения следующих моделей:

1. функциональной (IDEF0);
2. потоков данных (DFD);
3. реляционной базы данных (ERD).

Функциональная модель разрабатывается для точки зрения пользователя.

Целью моделирования является визуализация процесса шифрования.

# Глава 1. Функциональная модель (IDEF0)

Внешними входными информационными потоками процесса являются:

1. Данные пользователя.

Внешними выходными информационными потоками процесса являются:

1. Зашифрованные переданные данные.

Внешними управляющими потоками процесса являются:

1. ГОСТ 34.321-96.
2. IEEE 802.6.
3. Алгоритм ассиметричного шифрования

Основными механизмами процесса являются:

1. Модуль шифрования.

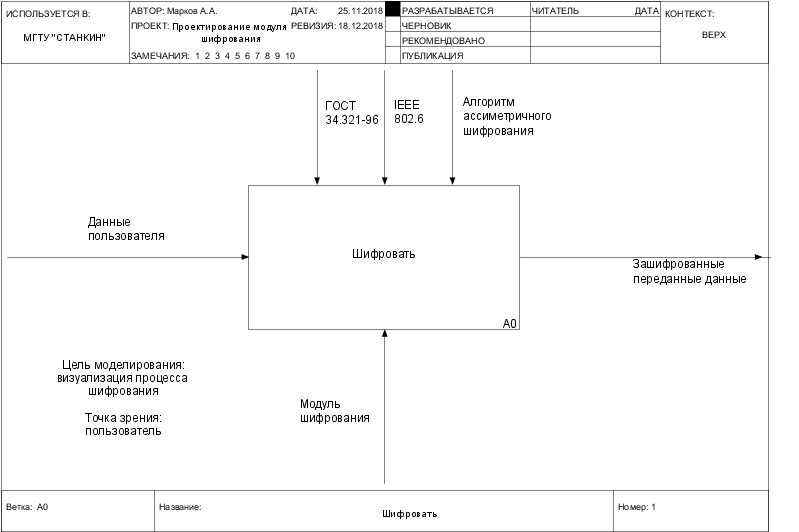


Рис. 1.1. Проектирование модуля шифрования

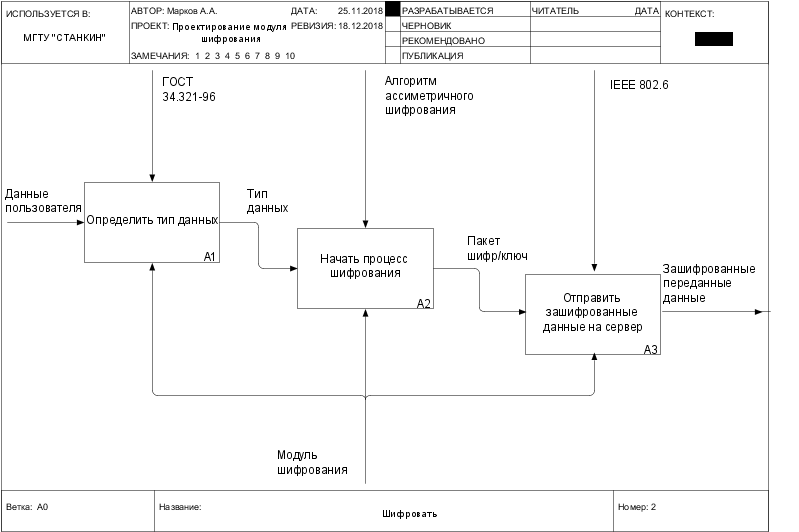


Рис. 1.2. Шифровать

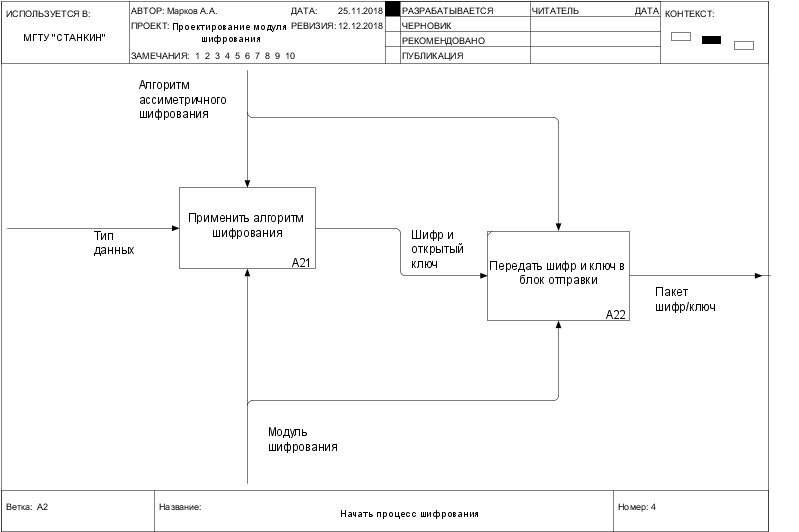


Рис. 1.3. Начать процесс шифрования

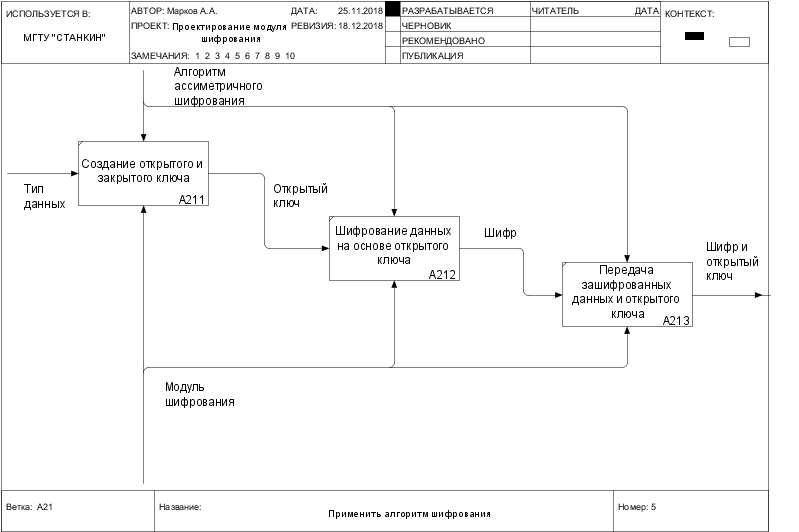


Рис. 1.4. Применить алгоритм шифрования

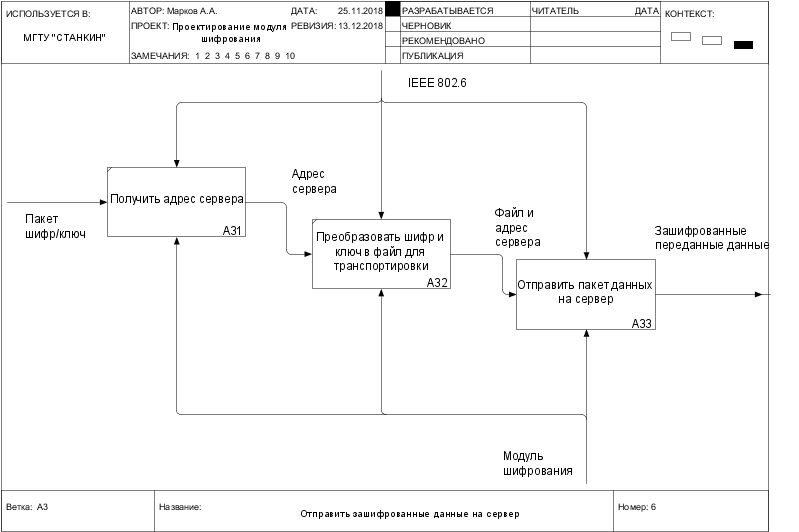


Рис. 1.5. Отправить зашифрованные данные на сервер

Показатели качества для автоматизируемых процессов следующие:

* Скорость шифрования.
* Надежность верификации.

Зависимость показателей качества от степени автоматизированности процессов прямо-пропорциональная.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Без системы** | **С системой** | **Выгода** |
| Применить алгоритм шифрования | От 15 минут до 24 часов | От нескольких секунд до 1 минуты | 15 минут минимум, 23 часа максимум |
| Отправить зашифрованные данные | 5 минут на то, чтобы запечатать зашифрованные данные и положить их в хранилище | 1-5 секунд (в зависимости от скорости соединения) на отправку зашифрованных данных на сервер | 295 секунд |

Определение числовых показателей для трудозатрат на разработку программных средств:

* Определение числа и сложности функциональных точек для модулей.
* Определение числа и сложности функциональных точек для хранилищ.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Форм | Данных | UFP |
| А1 | 0 | 1 | 7 |
| А2 | 0 | 0 | 0 |
| А3 | 0 | 1 | 7 |
|  |  |  | 14 |

* Расчет сложности разработки методом FPA/IFPUG.
  + VAF: 0,90
  + UFP: 14
  + DFP: 13
  + SLOC: 630
  + KLOC: 1
* Расчет трудозатрат на разработку «с нуля» методом COCOMO II.
  + PM: 1 чел/мес
  + TDEV: 3 мес

# Глава 2. Модель потоков данных (DFD)

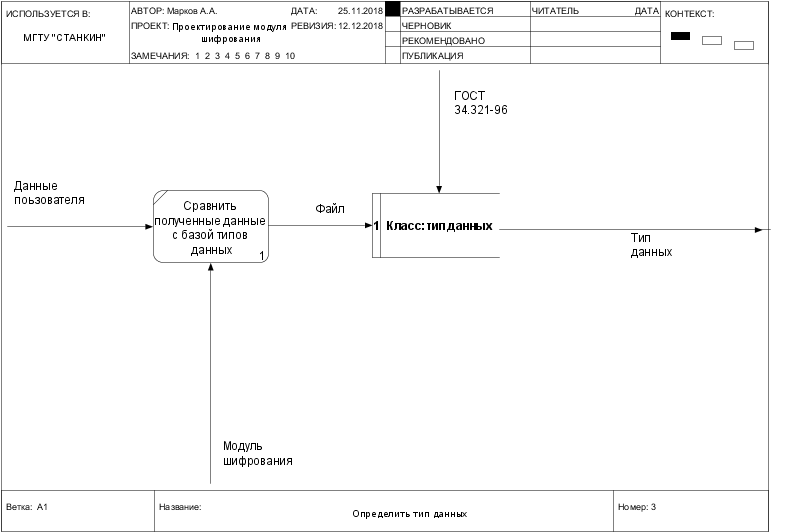


Рис. 2.1. Определить тип данных

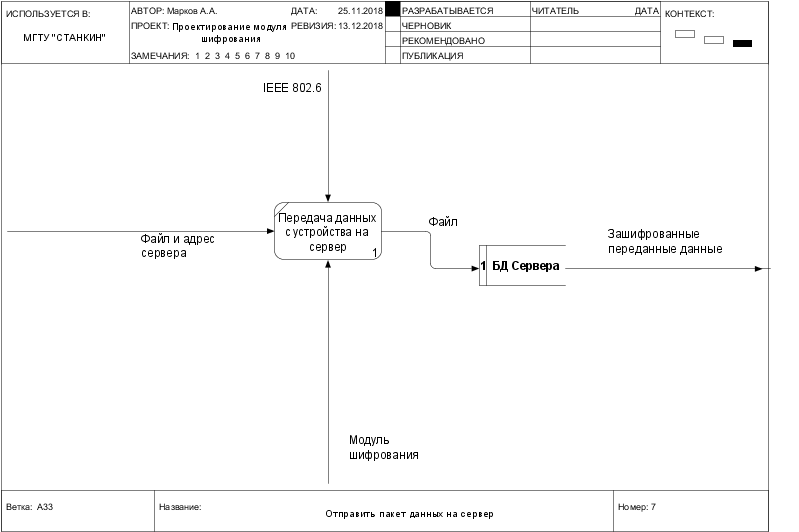


Рис. 2.2. Отправить данные на сервер

# Глава 3. Диаграммы классов (ERD)

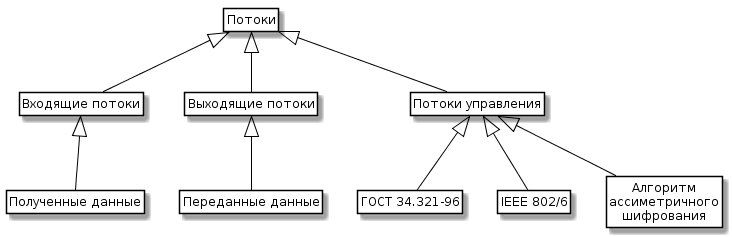


Рис. 3.1. Диаграмма потоков

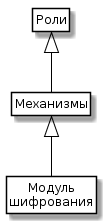


Рис. 3.2. Диаграмма ролей

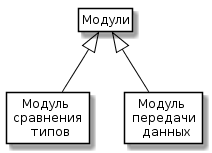


Рис. 3.3. Диаграмма модулей

# Заключение

В ходе данной работы был визуализирован процесс шифрования данных, а также выделены его основные характеристики. Использование автоматизации в данной сфере существенно ускорит процессы шифрования данных.

Был выполнен расчет сложности разработки методом FPA/IFPUG и показатели находятся на среднем уровне, что положительно влияет на скорость и эффективность работы над проектом.

Расчет трудозатрат на разработку «с нуля» методом COCOMO II показал примерное время разработки продукта, а именно за 3 месяца эту задачу выполнит 1 работник.