**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное ГОСУДАРСТВЕННОЕ бюджетное ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики

и вычислительной техники

Кафедра информационной

безопасности

**ОТЧЕТ**

**По Лабораторной работе №1**

**"ЗАПРОС НА ИДЕНТИФИКАЦИЮ / АУТЕНТИФИКАЦИЮ "**

Выполнил:

студент гр. БИс-32

Фомин Е.В.

Проверил:

Ассистент кафедры ИБ

Ситников И.В.

Йошкар-Ола

2017

**Ход работы**

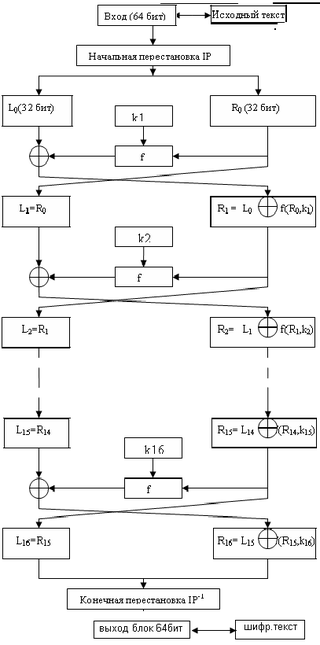
**Цель работы:** Ознакомиться с механизмами парольной защиты; методами идентификации и аутентификации; различными шифрами перестановки и методами их дешифрования.

Настоящая криптография (strong cryptography) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки и обеспечить конфиденциальность.

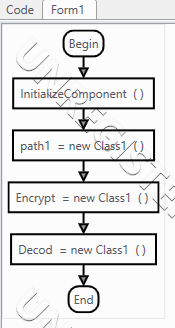
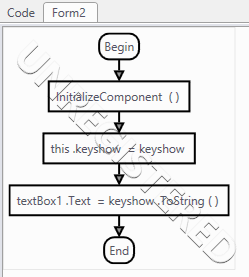
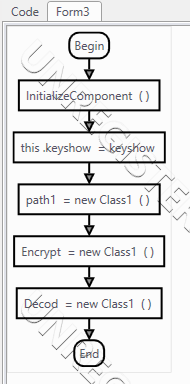
Изменение исходного текста так, чтобы скрыть от прочих его содер-жание, называют шифрованием (encryption). Зашифрованное сообщение называют шифротекстом (ciphertext). Процесс, при котором из шифро-текста извлекается открытый текст, называют дешифровкой (decryption). Обычно в процессе шифровки и дешифровки используется некий ключ (key), и алгоритм обеспечивает, что дешифрование можно сделать, лишь зная этот ключ.

*Ключ –* это конкретное секретное состояние некоторых параметров алгоритма преобразования данных, обеспечивающее выбор только од-ного варианта из всех возможных для данного алгоритма.

DES— алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 бита. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований.



Cхема шифрования алгоритма DES

**  **

**Вывод**

В ходе выполнения лабораторной работы были изучены следующие вопросы: механизмы парольной защиты; методами идентификации и аутентификации; метод шифрования DES и расшифрования.