Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информатики и веб-дизайна**

**Лабораторная работа №7**

исследование блочных шифров

Выполнил:

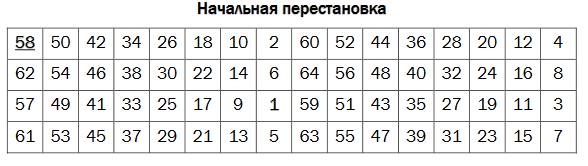
Студент 3 курса 10 группы ФИТ

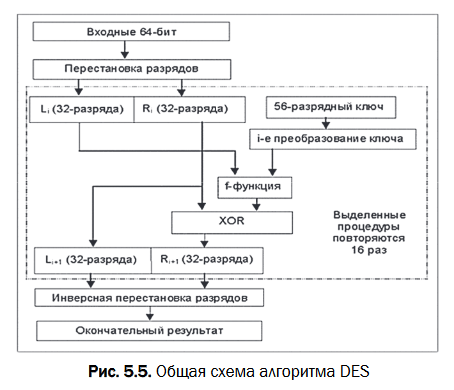
Баранчук Владислав Олегович

2021 г.

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров.

Алгоритм строится на основе сети Фейстеля. Входной блок данных, состоящий из 64 битов, преобразуется в выходной блок идентичной длины. В алгоритме широко используются рассеивания (подстановки) и перестановки битов текста, о которых мы упоминали выше. Комбинация двух указанных методов преобразования образует фундаментальный строительный блок DES, называемый раундом или циклом.





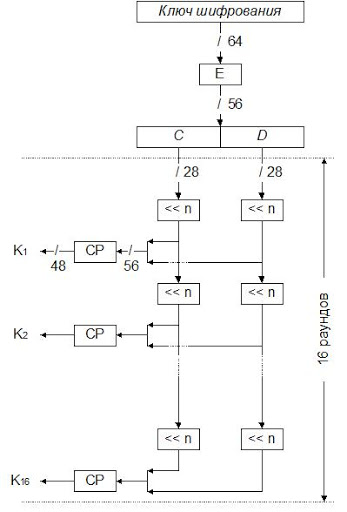


Схема f – функции

