**ФЕДЕРАЛЬНОЕ АГЕНСТВО СВЯЗИ  
Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича»  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Кафедра Защищенных систем связи  
Дисциплина «Основы криптографии»  
  
  
  
**Лабораторная работа №** **6  
  
  
Изучение и исследование блокового шифра AES**

**Вариант 4**Выполнил: ст. группы ИКТЗ-83  Громов А.А.

Проверил: Профессор кафедры ЗСС: д.т.н. проф. Яковлев В.А.

**Цель работы**

Изучить преобразования, выполняемые при шифровании и дешифровании сообщений в блоковом шифре AES, а также исследовать некоторые его свойства.

# Используемое программное обеспечение

Для выполнения работы используется специальная программа “AES.exe”