ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

«ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ» МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ

КАФЕДРА КОМП’ЮТЕРНИХ НАУК

Методичні вказівки

до виконання індивідуальної роботи з дисципліни «Основи криптології»

для студентів напряму підготовки «Інформатика» IV курсу денного відділення

*Тема індивідуальної роботи:* «Алгоритм блочного шифрування …». Назва алгоритму береться зі списку згідно отриманого варіанту.

*Метою* індивідуальної роботи є знайомство студентів з принципами роботи алгоритмів блочного шифрування та їх криптоаналізом.

*Звіт* з виконання індивідуальної роботи являє собою презентацію (у форматі Microsoft PowerPoint або OpenOffice Impress) обраного алгоритму блочного шифрування.

*Презентація* алгоритму повинна мати довільний дизайн та містити такі обов’язкові розділи:

1. П.І.поБ. упорядника презентації (студента), номер академічної групи.
2. Назва алгоритму, відомості про авторів.
3. Відношення для того чи іншого класу алгоритмів (наприклад мережа Фейстеля).
4. Можливі параметри алгоритму (довжина ключа та блоку вхідного).
5. Загальний опис алгоритму (у вигляді блок-схеми або покрокового опису).
6. Опис раунду алгоритму (у вигляді блок-схеми або покрокового опису).
7. Відомості про режими використання алгоритму.
8. Додаткові відомості, властиві саме цьому алгоритму (наприклад, розгортання ключа, розширення ключа, або щось інше).
9. Відомості про спроби криптоаналізу.

*Завдання до індивідуальної роботи.* У якості алгоритмів для реалізації системи шифрування тексту можна використовувати наступні блочні шифри:

1. Blowfish
2. IDEA
3. Camelia
4. Feal
5. Khufu
6. Serpent
7. Mars
8. Towfish
9. RC2 10.RC5 11.RC6 12.Khazad

**Рекомендовані джерела інформації**

1. Панасенко С.П. Алгоритмы шифрования. Специальный справочник .— Издательство: BHV-CПб, 2009 г., —576 стр