Доброго всем антивирусного здоровья!

Тема очередной лекции по дисциплине КМЗИ (03.04.20):

*Блочные шифры*. *Алгоритмы* 3DES, Blowfish, IDEA, Lucifer, [ГОСТ 28147-89](https://wiki2.org/ru/%D0%93%D0%9E%D0%A1%D0%A2_28147-89)

Методические материалы:

* Книга «Защита информации методами криптографии, стеганографии и обфускации», гл. 5, пп. 5.1-5.3,
* Рабочие методические материалы: Лабораторный практикум, ч. 2, теоретическая часть к лабораторной работе №5,
* Файл 10 Симметричная криптография1.pdf
* Книга Б. Шнайера: Прикладная криптография, (см. главы 13-14, файл SHnaier\_Brus\_Prikladnaya\_kriptografiya.\_Protokoly\_algoritmy\_i\_ishodnye\_teksty\_na\_yazyke\_S\_Litmir.net\_266719\_original\_ad9f9)

(все – на Diskstation, в папке *Урбанович/КМЗИ*).

Там же размещены материалы к лабораторной работе 8: Исследование асимметричных шифров RSA и Эль-Гамаля

П.Урбанович