Доброго всем антивирусного здоровья!

**Темы очередной лекции по дисциплине КМЗИ** (17.04.20):

- Потоковый шифр RC4.

- Основы асимметричной криптографии. Алгоритм Диффи-Хеллмана. Криптостойкость алгоритма. Атака «Человек *посередине*» (Man- in- the Middle)

Методические материалы:

- Рабочие методические материалы: Лабораторный практикум, ч. 2, теоретическая часть к лабораторной работе №6, (файл *лабораторный практикум ч2.pdf*),

- Книга «Защита информации методами криптографии, стеганографии и обфускации», п. 5.4.1 (файл *книга криптография .pdf*),

- презентация-файл *11 Асимметричная криптография.pdf*

- Книга Б. Шнайера, п. 17.1 и 19.1

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

**Выполнить задание!!!!**

**Последний срок – 19 апреля**

1. В чем состоит особенность сложения чисел по модулю 2n?

2. Сложить по модулю 102 пары чисел:

55 и 14; 76 и 24; 99 и 99.

3.Сложить по модулю 28:

двоичные числа 10101100 и 11001010; 01111111 и 01101101;

шестнадцатеричные числа 0В5 и 37.

Выполненные задания 1-3

*а также*

ранее выполненные Письменно (!!!) задания 7-8 (из вопросов для контроля и самоконтроля) к ЛР 6

все студенты группы пересылают (форма: электронный документ в текстовом формате или отсканированный рукописный текст) старосте группы, который создает архив и пересылает его на мой адрес ([pav.urb@yandex.by](mailto:pav.urb@yandex.by)) не позднее 20.04.

Буду обращать внимание на самостоятельность выполнения задания.

**Задание – часть коллоквиума!**

!!! Информация для участников конференции

Мы договорились о предоставлении мне до 15.04 (для редактирования) материалов в виде тезисов доклада , которые вы собирались докладывать на НТК.

П.Урбанович