

Код: група А „Криптография и защита на данните”

ECTS кредити: 5

Форма за оценяване: Изпит

Водещо звено:

Катедра: *СОФТУЕРНИ И ИНТЕРНЕТ ТЕХНОЛОГИИ*

*ФАКУЛТЕТ ПО ИЗЧИСЛИТЕЛНА ТЕХНИКА И АВТОМАТИЗАЦИЯ*

Седмичен хорариум: 2-0-2

Форма на контрол: Изпит - тест

Лектор: доц. д-р Златка Матева

Катедра: *СОФТУЕРНИ И ИНТЕРНЕТ ТЕХНОЛОГИИ*

тел. 0878-148-188

e-mail: ziz@abv.bg

Анотация: Дисциплината е избираема и има за цел да даде на студентите познания и умения по проблемите на защитата на данните срещу несанкциониран достъп в компютърните системи и мрежи. Разглеждат се механизмите за защита и тяхното обединяване в интегрирана система, задачата за проектиране на системата за защита, както и оценка на ефективността на отделните механизми за защита. Значително внимание се отделя на криптографските методи и средства. Изучават се основните подходи на съвременния криптоанализ, класификации на криптографските алгоритми и режими на използване, характерни класически и съвременни шифри, проблеми на програмната реализация и проектирането на високоскоростни криптографски алгоритми. Специално внимание се обръща на защитата на данните в Интернет.

Нужно е студентите да са запознати предварително с предаването на данни, компютърни мрежи, операционни системи, технология на програмирането и елементи на дискретната математика и комбинаториката.

Осъществява се паралелна връзка с администрирането на локални и Интернет мрежи.

Основни раздели на съдържанието:

- Криптоанализ
- криптографски алгоритми
- защита на данните

Форма на изнасяне на учебното съдържание: Учебното съдържание се представя чрез лекции и лабораторни упражнения и се затвърждава чрез индивидуална самостоятелна работа. Поднасяните теоретични знания по време на лекции са придружени с практически примери, а в лабораторните упражнения се реализират конкретни задачи.