Код: 44/45/46-10 „Криптография и защита на данните”

ECTS кредити: 6	Седмичен хорариум: 2-0-2
Форма за оценяване: Изпит	Форма на контрол: Изпит - тест

Водещо звено:

Катедра: *СОФТУЕРНИ И ИНТЕРНЕТ ТЕХНОЛОГИИ*
ФАКУЛТЕТ ПО ИЗЧИСЛИТЕЛНА ТЕХНИКА И АВТОМАТИЗАЦИЯ

Лектор: гл. ас. д-р Диян Динев

Катедра: *СОФТУЕРНИ И ИНТЕРНЕТ ТЕХНОЛОГИИ*

тел. 0899-904-956

e-mail: diyandinev@tu-varna.bg

Анотация:

Дисциплината е избираема и има за цел да даде на студентите знания 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. Основно внимание се отделя на криптографските алгоритми и на криптоанализа. Изучават се основните подходи на съвременния криптоанализ, класификации на криптографските алгоритми и режими на използване, характерни класически и съвременни шифри. Изучават се методи и средства на стеганографията за предаване на маскирани съобщения в изображения и звук.

Основни раздели в съдържанието:

1. Криптография – понятия и определения;
2. Секретни системи. Стеганография;
3. Поточни шифри – OTP, LFSR и др;
4. Блокови шифри - DES, Rijndael, 3DES и др;
5. Криптанализ на блокови шифри;
6. Асиметрична криптография;
7. Хеш функции;
8. Криптоанализ;
9. Защита на данните;

Форма на изнасяне на учебното съдържание:

Учебното съдържание се представя под формата на лекции и упражнения. Разясняват се теоретичните основи на криптографията и защитата на данни. По време на лабораторните упражнения се решават конкретни практически задачи.