

Код: 01, Блок В; дисц. **"КРИПТОГРАФИЯ И ЗАЩИТА НА ДАННИТЕ"**

Кредити: 20

Седмичен хорариум 2+0

Форма на контрол: изпит.

Форма за оценяване: писмен със събеседване

Водещо звено:

Катедра: „СИТ”

Факултет:ФИТА

Лектор: доц.д-р Златка Матева

катедра „СИТ”; тел. 052 - 383 - 228

Анотация:

Дисциплината има за цел да задълбочи знанията на докторантите в областта на криптографията и 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.

Основни раздели на съдържанието:

- Обзор на проблемите за защита на данните срещу несанкциониран достъп в компютърните системи и мрежи
- Политика в областта на криптографията
- Класическа криптография - примери за класически и комбинирани криптографски алгоритми
- Поточни шифри
- Блокови шифри
- Асиметрични криптографски алгоритми
- Хеш-функции
- Проблеми на реализацията и проектирането на високоскоростни софтуерни криптографски алгоритми. Оценка на бързодействието и статистически анализ на криптографските алгоритми
- Възможни проблеми с криптографската защита
- Класификация на съвременните автентикационни схеми
- Защита на предаваните данни в Интернет
- Защита на електронната търговия в Интернет
- Защита на електронната търговия в Интернет.

Форма на изнасяне на учебното съдържание:

Учебното съдържание се изнася под формата на лекции или под формата на консултации с докторанта, илюстрирани с примери, заедно с поставяне на задачи за самостоятелно изпълнение от страна на докторанта.