Студијски програм/студијски програми : Телекомуникације

Врста и ниво студија: основне струковне студије

**Назив предмета: Сигурност на Интернету**

Статус предмета: изборни

Број ЕСПБ: 4

Услов: нема

**Циљ предмета**

Упознавање са алгоритмима, техникама и протоколима обезбеђивања сигурности информација и мрежних ресурса на Интернету.

**Исход предмета**

Очекује се да студент може да самостално обезбеди заштиту података и ресурса мреже од неовлашћеног приступа и злоупотребе, применом сигурносних протокола у којима су имплементирани криптографски алгоритми и технике електронског потписивања.

**Садржај предмета**

*Теоријска настава*

Упознавање са проблемима сигурности информација и мрежних ресурса на Интернету. Системи и технике заштите тајности података. Симетрични криптосистеми: DES, 3DES и IDEA. Хеш алгоритми: MD5 и SHA-1. Асиметрични криптосистеми: Diffi-Hellman-ова размена експоненцијалног кључа, RSA криптосистем са јавним кључем. Инфраструктура PKI система: технике електронског потписивања, електронски сертификати, сертификациона тела. Сигурносни протоколи: IPSec, SSL, PGP, S/MIME, SET. Заштитни зидови.

*Практична настава:Вежбе, Други облици наставе, Студијски истраживачки рад*

Демонстрација коришћења GPG4Win софтвера за генерисање јавног и тајног кључа, шифровање и аутентификовање корисника у комуникацији електронском поштом.

**Литература**


1. Д. Певац, *Сигурност на Интернету*, уџбеник, Висока ICT школа, Београд, 2010.
2. M. Y. Rhee, *Internet Security*, John Wiley & Sons Ltd, England, 2003.