

Студијски програм/студијски програми : Интернет технологије – модул Web програмирање, модул Администрирање рачунарских мрежа, модул Медицинска информатика
Врста и ниво студија: основне струковне студије
<b>Назив предмета: Сигурност на Интернету</b>
Статус предмета: изборни, изборни, изборни
Број ЕСПБ: 4
Услов: нема
<b>Циљ предмета</b> Упознавање са алгоритмима, техникама и протоколима обезбеђивања сигурности информација и мрежних ресурса на Интернету.
<b>Исход предмета</b> 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.
<b>Садржај предмета</b> <i>Теоријска настава</i> 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. <i>Практична настава: Вежбе, Други облици наставе, Студијски истраживачки рад</i> Демонстрација коришћења GPG4Win софтвера за генерисање јавног и тајног кључа, шифровање и аутентификовање корисника у комуникацији електронском поштом.
<b>Литература</b> 1. Д. Певац, <i>Сигурност на Интернету</i> , уџбеник, Висока ICT школа, Београд, 2010. 2. М. Y. Rhee, <i>Internet Security</i> , John Wiley & Sons Ltd, England, 2003.