INFORMACIJA ZA STUDENTE I PLAN RADA

	Naziv predmeta:	*Bezbjednost računarskih sistema*		
Šifra predmeta	***Status predmeta***	***Semestar***	***Broj ECTS kredita***	***Fond časova***
	obavezni	**II**	**5**	**3+0V**

Studijski programi za koje se organizuje : Specijalističke studije, primenjeni studijski program RAČUNARSTO I INFORMACIONE TEHNOLOGIJE.
Uslovljenost drugim predmetima: nema uslovljenosti
Ciljevi izučavanja predmeta: Upoznavanje studenata sa prijetnjama bezbjednosti u računarskim sistemima i načinima, oblicima i metodama zaštite računarskih sistema. Izučavanje algoritama korišćenih za šifriranje informacija. Upoznavanje sa praktičnom primjenom kriptografije u oblasti zaštite računarskih sistema, zaštitom elektronske pošte, web-a i transakcija, kao i savremenom zaštitom na mrežnom nivou.
Ime i prezime nastavnika i saradnika: *Prof. dr Stevan Šćepanović - predavanja*
Metod nastave i savladanja gradiva: Predavanja i demonstracije u računarskoj učionici / laboratoriji. Učenje i samostalna izrada praktičnih zadataka. Konsultacije.

PLAN RADA

Nedjelja i datum	*Naziv metodskih jedinica za predavanja(P), vježbe (V) i ostale nastavne sadržaje O); Planirani oblik provjere znanja(PZ: domaći zadaci, kontrolni testovi, kolokvijumi, ...)*	
Pripremna nedjelja		
I - 10.02.20.	***Predavanja***	Uvod. Osnovni pojmovi o bezbjednosti u računarskim sistemima.
II - 17.02.20.	***Predavanja***	Prijetnje bezbjednosti u računarskim sistemima i principi izgradnje bezbjednog računarskog sistema.
III - 24.02.20.	***Predavanja***	Degradacija sistema pomoću virusa i drugih štetnih programa. Preventivna zaštita računara od virusa. Antivirus programi.
IV - 2.03.20.	***Predavanja***	Neophodna zaštita računarskih sistema, politika i mehanizmi zaštite. Osnovni pojmovi iz kriptografije i kriptoanalize. Klasifikacija kriptosistema.
V - 10.03.20.	***Predavanja***	Simetrično ili klasično šifriranje. Apsolutno sigurna šifra. Konfuzija i difuzija i osnovni principi šifriranja. Blokovske šifre. Šifrovanje premještanjem i zamjenom.
VI - 16.03.20.	***Prov. zn.***	**I Kolokvijum.**
VII - 24.03.20.	***Predavanja***	*Fajstelova* šifra. DES standard šifriranja podataka. Trojno šifrovanje. Otvaranje DES šifri. Ostale simetrične šifre.
VIII- 30.03.20.	***Predavanja***	AES - napredni standard šifriranja. *Rijndael*-ova šifra. Pouzdanost korišćenja simetričnih šifri. Lokacija i razmještaj funkcija i uređaja za šifriranje. Algoritmi sa otvorenim ključevima. Algoritam RSA.
IX - 6.04.20.	***Predavanja***	Protokoli za provjeru i principi izgradnje protokola autentičnosti. Autentičnost na osnovu dijeljenog ključa. Instalacija dijeljenog ključa i *Difi-Helmanov* protokol za razmjenu ključeva.
X - 13.04.20.	***Predavanja***	Provjera originalnosti kroz centar za distribuciju ključeva i Protokol *Nidhema-Šredera* za provjeru autentičnosti. Utvrđivanje originalnosti protokolom Kerber.
XI - 27.04.20.	***Predavanja***	Elektronski potpis sa tajnim ključem i elektronski potpis sa otvorenim ključem. *Hash* funkcije. Generacija Message Digest korišćenjem SHA-1. Elektronska uvjerenja. Kontrola pristupa i autorizacija kao mehanizam zaštite. Zaštita elektronske pošte (PGP operacije i zaštitno višenamjensko Internet Mail proširenje - S/MIME).

XIII - 4.05.20.	***Predavanja***	Zaštita Web-a (SSL Protokol i Internet TLS standard). Zaštita elektronskih transakcija. Zaštita na mrežnom nivou i IP zaštita. Transportni i tunelski režim zaštite, AH i ESP. Virtuelne privatne mreže i tunelovanje. Zaštitna barijera (firewall).
XIV - 11.05.20.	***Prov. zn.***	**II Kolokvijum.**
XV - 18.05.20.	***Prov. zn.***	**Popravni kolokvijum**
XVI-XVI - 25.05.20.-7.06.20.		**ZAVRŠNI ISPIT**
XVII-XIX - 8.06.20.-16.06.20		**Popravni završni ispit**

Obaveze studenta u toku nastave: Studenti su obavezni da aktivno prate nastavu, rade oba kolokvijuma i sve planom predviđene vježbe.

Konsultacije: Utorkom poslije predavanja.

Opterećenje studenta u časovima: 5 kredita x 30 sati = 150 sati

nedjeljno	u semestru
5 kredita x 40/30 = 6 sati i 40 minuta **Predavanja: 3** sata **Ostale nastavne aktivnosti: 0** **Individualni rad studenata**: **3** sata i **40** minuta.	**Nastava i završni ispit**: : (6 sati i 40 minuta) x16 = **106 sati i 40 minuta**. **Neophodne pripreme** (administracija, upis, ovjera prije početka semestra) 2 x (6 sati i 40 minuta) = **13 sati i 20 minuta** **Ukupno opterećenje za predmet:** 5x30 = **150 sati** **Dopunski rad:** za pripremu ispita u popravnom ispitnom roku, uključujući i polaganje popravnog ispita od 0 do **30 sati** (preostalo vrijeme od prve dvije stavke do ukupnog opterećenja za predmet 150 sati) **Struktura opterećenja**: 106 sati i 40 minuta (Nastava i završni ispit)+13 sati i 20 minuta (priprema)+30 sati (dopunski rad)

Literatura:

- M. Strib, Č. Perkins - "Firewalls zaštita od hakera", Kompjuter biblioteka, "Svetlost", Čačak, 2003.
- S. McClure, J. Scambray, G. Kurtz - "Sigurnost na mreži", Kompjuter biblioteka, "Svetlost", Čačak, 2001.
- W. Stallings, - "Cryptography and Network Security.", Prentice-Hall, Inc., New Jersey, 1999.

Oblici provjere znanja i ocjenjivanje:

- Dva kolokvijuma se ocijenjuju ukupno sa 70 poena.
- Završni ispit 30 poena.
- Prelazna ocjena se dobija ako se kumulativno sakupi najmanje 50 poena.

Ocjena	***A***	***B***	***C***	***D***	***E***
Broj poena	***90-100***	***80-89***	***70-79***	***60-69***	***50-59***

Posebne naznake za predmet:

Napomena: