

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 - 12.02.18.	Predavanja Uvod. Osnovni pojmovi o bezbjednosti u računarskim sistemima.
II - 19.02.18.	Predavanja Prijetnje bezbjednosti u računarskim sistemima i principi izgradnje bezbjednog računarskog sistema.
III - 26.02.18.	Predavanja Degradacija sistema pomoću virusa i drugih štetnih programa. Preventivna zaštita računara od virusa. Antivirus programi.
IV - 5.03.18.	Predavanja Neophodna zaštita računarskih sistema, politika i mehanizmi zaštite. Osnovni pojmovi iz kriptografije i kriptanalize. Klasifikacija kriptosistema.
V - 12.03.18.	Predavanja Simetrično ili klasično šifriranje. Apsolutno sigurna šifra. Konfuzija i difuzija i osnovni principi šifriranja. Blokofske šifre. Šifrovanje premještanjem i zamjenom.
VI - 19.03.18.	Prov. zn. I Kolokvijum.
VII - 26.03.18.	Predavanja Fajstelova šifra. DES standard šifriranja podataka. Trojno šifrovanje. Otvaranje DES šifri. Ostale simetrične šifre.
VIII - 2.04.18.	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 - 9.04.18.	Predavanja Protokoli za provjeru i principi izgradnje protokola autentičnosti. Autentičnost na osnovu dijeljenog ključa. Instalacija dijeljenog ključa i Difi-Helmanov protokol za razmjenu ključeva. Provjera originalnosti kroz centar za distribuciju ključeva i Protokol Nidhema-Šredera za provjeru autentičnosti. Utvrđivanje originalnosti protokolom Kerber.
XI - 23.04.18.	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 - 30.05.18.	<i>Predavanja</i>	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 - 7.05.18.	<i>Prov. zn.</i>	II Kolokvijum.			
XV - 14.05.18.	<i>Prov. zn.</i>	Popravni kolokvijum			
XVI-XVII-30.05.18-11.06.18		ZAVRŠNI ISPIT			
XVIII-XIX-13.06.18-25.06.18		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			Nastava i završni ispit: : (6 sati i 40 minuta) x16 = 106 sati i 40 minuta.		
Predavanja: 3 sata			Neophodne pripreme (administracija, upis, ovjera prije početka semestra) 2 x (6 sati i 40 minuta) = 13 sati i 20 minuta		
Ostale nastavne aktivnosti: 0			Ukupno opterećenje za predmet: 5x30 = 150 sati		
Individualni rad studenata: 3 sata i 40 minuta.			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:					
<ul style="list-style-type: none"> - 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:					
<ul style="list-style-type: none"> - Dva kolokvijuma se ocjenjuju 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:					