

Prirodno-matematički fakultet / Računarske nauke / BEZBJEDNOST RAČUNARSKIH SISTEMA

Naziv predmeta:	BEZBJEDNOST RAČUNARSKIH SISTEMA			
Šifra predmeta	Status predmeta	Semestar	Broj ECTS kredita	Fond časova (P+V+L)
2300	Obavezan	5	4	2+0+0
Studijski programi za koje se organizuje	Računarske nauke			
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.			
Ishodi učenja	Nakon što student položi ovaj ispit, biće u mogućnosti da: 1.Objasni pojam bezbjednog računarskog sistema. 2.Opiše moguće prijetnje i rizike ugrožavanja bezbjednosti računarskih sistema. 3.Opiše pojmove autentičnosti i autorizacije i protokole za njihovu realizaciju. 4.Ovlada sadržajima koji uključuju šifriranje i dešifriranje podataka, algoritme šifriranja i procedure zaštite. 5.Opiše metodologiju zaštite elektronske pošte, veba, elektronskog potpisa i elektronskog sertifikata. 6.Projektuje i implementira neophodnu zaštitu konkretnog računarskog sistema.			
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 i program rada				
Pripremne nedjelje	Priprema i upis semestra			
I nedjelja, pred.	Uvod. Osnovni pojmovi o bezbjednosti u računarskim sistemima.			
I nedjelja, vježbe				
II nedjelja, pred.	Prijetnje bezbjednosti u računarskim sistemima i principi izgradnje bezbjednog računarskog sistema.			
II nedjelja, vježbe				
III nedjelja, pred.	Degradacija sistema pomoću virusa i drugih štetnih programa. Preventivna zaštita računara od virusa. Antivirus programi.			
III nedjelja, vježbe				
IV nedjelja, pred.	Neophodna zaštita računarskih sistema, politika i mehanizmi zaštite. Osnovni pojmovi iz kriptografije i kriptanalize. Klasifikacija kriptosistema.			
IV nedjelja, vježbe				
V nedjelja, pred.	Simetrično ili klasično šifriranje. Apsolutno sigurna šifra. Konfuzija i difuzija i osnovni principi šifriranja. Blokvske šifre. Šifrovanje premještanjem i zamjenom.			
V nedjelja, vježbe				
VI nedjelja, pred.	Fajstelova šifra. DES standard šifriranja podataka. Trojno šifrovanje. Otvaranje DES šifri. Ostale simetrične šifre.			
VI nedjelja, vježbe				
VII nedjelja, pred.	I Kolokvijum.			
VII nedjelja, vježbe				
VIII nedjelja, pred.	AES - napredni standard šifriranja. Rijndael-ova šifra. Pouzdanost korišćenja simetričnih šifri. Lokacija i razmještaj funkcija i uređaja za šifriranje.			
VIII nedjelja, vježbe				
IX nedjelja, pred.	Algoritmi sa otvorenim ključevima. Algoritam RSA. Protokoli za provjeru i principi izgradnje protokola autentičnosti. Autentičnost na osnovu dijeljenog ključa.			
IX nedjelja, vježbe				
X nedjelja, pred.	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.			

X nedjelja, vježbe						
XI nedjelja, pred.	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.					
XI nedjelja, vježbe						
XII nedjelja, pred.	Zaštita elektronske pošte (PGP operacije i zaštitno višenamjensko Internet Mail proširenje - S/MIME). Zaštita Web-a (SSL Protokol i Internet TLS standard). Zaštita elektronskih transakcija.					
XII nedjelja, vježbe						
XIII nedjelja, pred.	Zaštita na mrežnom nivou i IP zaštita. Transportni i tunelski režim zaštite, AH i ESP. Virtuelne privatne mreže i tunelovanje. Zaštitna barijera (firewall).					
XIII nedjelja, vježbe						
XIV nedjelja, pred.	II Kolokvijum.					
XIV nedjelja, vježbe						
XV nedjelja, pred.	Popravni kolokvijum					
XV nedjelja, vježbe						
Opterećenje studenta	4 kredita x 30 sati = 120 sati					
Nedjeljno	U toku semestra					
4 kredita x 40/30=5 sati i 20 minuta 2 sat(a) teorijskog predavanja 0 sat(a) praktičnog predavanja 0 vježbi 3 sat(a) i 20 minuta samostalnog rada, uključujući i konsultacije	Nastava i završni ispit: 5 sati i 20 minuta x 16 =85 sati i 20 minuta Neophodna priprema prije početka semestra (administracija, upis, ovjera): 5 sati i 20 minuta x 2 =10 sati i 40 minuta Ukupno opterećenje za predmet: 4 x 30=120 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) 24 sati i 0 minuta Struktura opterećenja: 85 sati i 20 minuta (nastava), 10 sati i 40 minuta (priprema), 24 sati i 0 minuta (dopunski rad)					
Obaveze studenta u toku nastave	Studenti su obavezni da aktivno prate nastavu, predaju domaće zadatke, rade oba kolokvijuma i urade sve planom predviđene vježbe.					
Konsultacije	Svake nedelje poslije predavanja.					
Literatura	1. M. Strib, Č. Perkins - "Firewalls zaštita od hakera", Kompjuter biblioteka, "Svetlost", Čačak, 2003. 2. S. McClure, J. Scambray, G. Kurtz - "Sigurnost na mreži", Kompjuter biblioteka, "Svetlost", Čačak, 2001. 3. W. Stallings, - "Cryptography and Network Security.", Prentice-Hall, Inc., New Jersey, 1999.					
Oblici provjere znanja i ocjenjivanje	Dva kolokvijuma se ocjenjuju ukupno sa 70 poena. Završni ispit 30 poena. Prelazna ocjena se dobija ako se kumulativno sakupi najmanje 50 poena.					
Posebne naznake za predmet						
Napomena						
Ocjena:	F	E	D	C	B	A
Broj poena	manje od 50 poena	više ili jednako 50 poena i manje od 60 poena	više ili jednako 60 poena i manje od 70 poena	više ili jednako 70 poena i manje od 80 poena	više ili jednako 80 poena i manje od 90 poena	više ili jednako 90 poena