

**Elektrotehnički fakultet / Primijenjeno računarstvo / Bezbjednost i zaštita informacionih sistema**

Uslovljeno drugim predmetima	Nema.
Ciljevi izučavanja predmeta	Kroz ovaj predmet studenti se upoznaju sa osnovnim elementima koji utiču na sigurnost mreža i aplikacija, tehničkim, organizacionim i ljudskim faktorima povezanim sa rizicima informacione sigurnosti. Cilj je i ovladavanje procjenom rizika informacione sigurnosti, kao i upoznavanje sa metodama osiguravanja mreža i aplikacija.
Ime i prezime nastavnika i saradnika	Prof. dr Nikola Žarić
Metod nastave i savladanja gradiva	Predavanja i vježbe u računarskoj učionici / laboratoriji. Učenje i samostalna izrada praktičnih zadataka. Konsultacije.
I nedjelja, pred.	Prijetnje, napadi, sigurnost i metode zaštite
I nedjelja, vježbe	Praktični primjeri sigurnosnih rizika
II nedjelja, pred.	Sigurnosne arhitekture i modeli
II nedjelja, vježbe	Analiza primjera sigurnosnih arhitektura i modela
III nedjelja, pred.	Kontrola pristupa i mrežne barijere
III nedjelja, vježbe	Primjeri konfiguracije kontrole pristupe i mrežnih barijera
IV nedjelja, pred.	Sistemi za otkrivanje i sprečavanje upada
IV nedjelja, vježbe	Analiza i upotreba sistema za otkrivanje i sprečavanje upada
V nedjelja, pred.	Elektronsko poslovanje i sigurnost na Internetu
V nedjelja, vježbe	Upotreba alata za elektronsko poslovanje
VI nedjelja, pred.	Sigurnost bežičnih i mobilnih mreža
VI nedjelja, vježbe	Primjeri sigurnosnih rizika u bežičnim i mobilnim mrežama
VII nedjelja, pred.	I kolokvijum
VII nedjelja, vježbe	I kolokvijum
VIII nedjelja, pred.	Sigurnost i zaštita operativnih sistema
VIII nedjelja, vježbe	Konfiguracija sigurnosti i zaštite operativnih sistema
IX nedjelja, pred.	Sigurnost baza podataka
IX nedjelja, vježbe	Programiranje zaštite sigurnosti baza podataka
X nedjelja, pred.	Sigurnosni aspekti programiranja
X nedjelja, vježbe	Kreiranje koda za zaštitu na aplikativnom nivou
XI nedjelja, pred.	Nadzor računarskih mreža
XI nedjelja, vježbe	Upotreba alata za nadzor računarskih mreža
XII nedjelja, pred.	Organizacione, fizičke i pravne metode zaštite, društveni aspekti
XII nedjelja, vježbe	Praktični primjeri i analiza
XIII nedjelja, pred.	Planiranje održanja kontinuiteta posla i oporavka od nesreća
XIII nedjelja, vježbe	Kreiranje plana održavanja i oporavka od nesreće
XIV nedjelja, pred.	Etičko hakerisanje i ispitivanje mogućnosti probaja
XIV nedjelja, vježbe	Upotreba alata za etičko hakerisanje
XV nedjelja, pred.	Popravak kolokvijuma
XV nedjelja, vježbe	Popravak kolokvijuma
Obaveze studenta u toku nastave	Redovno prisustvo nastavi, primjerno vladanje, pohađanje provjera znanja (kolokvijum i završni ispit).
Konsultacije	Nakon predavanja, a po potrebi po dogovoru.
Opterećenje studenta u casovima	Nastava i završni ispit: (6 sati i 40 minuta) x 15 = 100 sati Neophodne pripreme prije početka semestra (administracija, upis, ovjera) 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 36 sati i 40 minuta (preostalo vrijeme od prve dvije stavke do ukupnog opterećenja za predmet 150 sati) Struktura opterećenja: 100 sati (Nastava) + 13h i 20m (Priprema) + 36 sati i 40 minuta (Dopunski rad)
Literatura	Skripta sa predavanja J. Andress, „The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice“, Syngress, 2 edition, June 2014
Oblici provjere znanja i ocjenjivanje	Laboratorijske vježbe 10x1 ukupno 10 poena Kolokvijum ukupno 40 poena Završni ispit ukupno 50 poena Prelazna ocjena (A-E) se dobija ako se kumulativno sakupi najmanje 50 poena.
Posebne naznake za predmet	
Napomena	
Ishodi učenja	Nakon što student položi ovaj ispit biće u mogućnosti da: 1) Identificuje ključne elemente koji utiču na sigurnost mreža i aplikacija; 2) Objasni tehničke, organizacione i ljudske faktore koji su povezani sa rizicima informacione sigurnosti; 3) Objasni potrebu za implementacijom sigurnosnih mehanizama; 4) Procijeni rizike informacione sigurnosti; 5) Opiše metode i postupke osiguravanja sigurnosti mreža i aplikacija; 6) Identificuje sigurnosne zahtjeve mreža i aplikacija; 7) Analizira prednosti i nedostatke sigurnosnih mehanizama.