SVEUČILIŠTE U RIJECI
FAKULTET INFORMATIKE I DIGITALNIH TEHNOLOGIJA
Radmile Matejčić 2, Rijeka

Akademska godina 2022./2023.

OSNOVNI PODACI O PREDMETU		
Naziv predmeta	Sigurnost informacijskih i komunikacijskih sustava	
Studijski program	Sveučilišni prijediplomski studij Informatika	
Status predmeta	obvezatan	
Semestar	4.	
Bodovna vrijednost i način izvođenja nastave	ECTS koeficijent opterećenosti studenata	5
	Broj sati (P+V+S)	30+30+0
Nositelj predmeta	izv. prof. dr. sc. Božidar Kovačić	
E-mail	bkovacic@inf.uniri.hr	
Ured	O-414	
Vrijeme konzultacija	Petkom od 12:00 do 13:00 uz prethodni dogovor e-mailom	
Asistent	Milan Petrović	
E-mail	milan.petrovic@inf.uniri.hr	
Ured	O-522	
Vrijeme konzultacija	Utorkom od 14:00 do 16:00 uz prethodni dogovor e-mailom	

DETALJNI OPIS PREDMETA

Ciljevi predmeta

Cilj je predmeta usvajanje temeljnih znanja u području sigurnosti informacijskih sustava, upoznavanje s rizicima i prijetnjama informacijskim sustavima, metodama njihove zaštite, metodama enkripcije i dekripcije podataka te postupcima za mjerenje i vrednovanje postignute razine informacijske sigurnosti.

Uvjeti za upis predmeta

Odslušani predmeti Osnove informatike i Računalne mreže.

Očekivani ishodi učenja za predmet

Očekuje se da nakon izvršavanja svih programom predviđenih obveza studenti budu sposobni:
I1. Analizirati protokole u sigurnom i nesigurnom komunikacijskom kanalu.
I2. Definirati i objasniti razlike između protokola HTTP i HTTPS.
I3. Odrediti zaštitne funkcije informacijskog sustava, te izgraditi informacijski sustav s autentifikacijskim, autorizacijskim i dnevničkim modulima.
I4. Procijeniti rizike informacijske sigurnosti osobnih računala i poslužitelja te opisati načine izvođenja mogućih napada.
I5. Pojasniti načine zaštite informacijskog sustava od pojedinih vrsta napada na integritet podataka.

Sadržaj predmeta

- Sigurnosni rizici informacijskih sustava. Analiza i procjena rizika. Prijetnje sigurnosti i vjerojatnost njihova nastanka. Ranjivost informacijskih sustava.
- Sigurnosni incidenti informacijskih sustava. Prepoznavanje znakova sigurnosnih incidenata.
- Sigurnosni mehanizmi i kontrolni postupci, kriptografija, enkripcija i dekripcija podataka.
- Upravljanje, poboljšanje i nadzor sustava informacijske sigurnosti. Mjerenje učinkovitosti

kontrola. • Upravljanje sigurnosnim rizicima. Metode za procjenu rizika. Upravljanje rizikom kao instrument unaprjeđivanja sigurnosti.		
Vrsta izvođenja nastave	☒ predavanja	☒ samostalni zadaci
	☐ seminari i radionice	☒ multimedija i mreža
	☒ vježbe	☒ laboratorij
	☒ obrazovanje na daljinu	☐ mentorski rad
	☐ terenska nastava	☐ ostalo _____
Komentari	Nastava se izvodi kombinirajući rad u učionici i računalnom laboratoriju uz primjenu sustava za udaljeno učenje. Studenti će kod upisa kolegija biti upućeni na korištenje sustava za udaljeno učenje.	
Obavezna literatura (u trenutku prijave prijedloga studijskog programa)		
1. Dieter Gollman, "Computer Security", John Wiley & Sons, 2011. 2. Harold F. Tipton, Micki Krause, "Information Security Management", 6th Edition, Taylor & Francis Group, 2007. 3. Thomas R. Peltier, "Information Security Policies and Procedures: A Practitioner's Reference", Second Edition, 2004. 4. Wenliang Du, "Computer Security: A Hands-on Approach", Create Space, 2017.		
Dopunska literatura (u trenutku prijave prijedloga studijskog programa)		
1. Donald L. Pipkin, "Information Security", Prentice Hall PTR, 2000. 2. Thomas R. Peltier, "Information Security Risk Analysis", Third Edition, CRC Press, 2010.		
Načini praćenja kvalitete koji osiguravaju stjecanje izlaznih znanja, vještina i kompetencija		
Predviđa se periodičko provođenje evaluacije s ciljem osiguranja i kontinuiranog unapređenja kvalitete nastave i studijskog programa (u okviru aktivnosti Odbora za upravljanje i unapređenje kvalitete Fakulteta informatike i digitalnih tehnologija). U zadnjem tjednu nastave provodit će se anonimna evaluacija kvalitete održane nastave od strane studenata. Provest će se i analiza uspješnosti studenata na predmetu (postotak studenata koji su položili predmet i prosjek njihovih ocjena).		
Mogućnost izvođenja na stranom jeziku	Nema.	

OBVEZE, PRAĆENJE RADA I VREDNOVANJE STUDENATA

VRSTA AKTIVNOSTI	ECTS	ECTS - PRAKTIČNI RAD	ISHODI UČENJA	SPECIFIČNA AKTIVNOST	METODA PROCJENJIVANJA	BODOVI MAX.
Pohađanje nastave i aktivnosti u nastavi	1,5	1	I1–I5	Prisutnost studenata i odgovaranje na pitanja nastavnika	Popisivanje (evidencija)	0
Pisani ispit	1	0,7	I1, I2	Kolokvij iz dijela gradiva predavanja	Ovisno o stupnju točnosti i potpunosti	25
Kontinuirana provjera znanja	1	0,8	I1, I2	Kontrolna zadaća iz dijela gradiva vježbi	Ovisno o stupnju točnosti i	25

VRSTA AKTIVNOSTI	ECTS	ECTS - PRAKTIČNI RAD	ISHODI UČENJA	SPECIFIČNA AKTIVNOST	METODA PROCJENJIVANJA	BODOVI MAX.
					potpunosti	
Projekt (dio)	0,5	0,8	I3	Određivanje zaštitne funkcije informacijskog sustava te izrada ili konfiguracija model autentifikacije i autorizacije korisnika za zadanu aplikaciju	20 bodova prema definiranim kriterijima	20
Završni ispit	1	0	I3, I4, I5	Analiza rizika i upravljanje razinom usluga, incidentima, problemima, zahtjevima i raspoloživošću	30 bodova prema definiranim kriterijima	30
UKUPNO	**5**	**3,3**				**100**

Obveze i vrednovanje studenata

Pohađanje nastave i aktivnosti u nastavi

Studentice i studenti su dužni redovito pohađati predavanja i vježbe predmeta o čemu predmetni nastavnik i asistent vode evidenciju. Od studentica i studenata očekuje se aktivno sudjelovanje u aktivnostima tijekom predavanja (npr. diskusija ili rješavanje problemskih zadataka) i vježbi (npr. rješavanje praktičnih zadataka na računalu, predaja rješenja zadataka ili priprema za vježbe čitanjem pripremljenih materijala). Studentice i studenti koji ne prisustvuju barem 70% od ukupnog fonda sati predavanja i isto toliko vježbi (uključujući i *online* predavanja i vježbe, izvedene sinkronim pristupom), ne mogu pristupiti završnome ispitu predmeta. U slučaju opravdanog izostanka studentice i studenti su dužni, u roku od najviše 7 dana od izostanka, donijeti valjanu (liječničku) ispričnicu. Također, studentice i studenti trebaju redovito pratiti aktivnosti predmeta u okviru sustava za udaljeno učenje Merlin (https://moodle.srce.hr/). Ova se aktivnost ne boduje ocjenskim bodovima.

Pisani ispit

Tijekom semestra pisat će se kolokvij koji će uključivati teorijska pitanja iz dijela sadržaja predavanja. Na kolokviju student će moći sakupiti najviše 25 ocjenskih bodova.

Kontinuirana provjera znanja

Tijekom semestra bit će održano pet laboratorijskih vježbi koje će uključivati korištenje algoritama za šifriranje u okviru nekoliko gotovih aplikacija (sigurna ljuska, VPN klijent i poslužitelj, web klijent i poslužitelj te sustav za upravljanje bazom podataka) na računalu prema danim uputama. Laboratorijske vježbe se izvode tako da student unaprijed dobiva nastavne materijale i zadatke za samostalnu pripremu putem sustava za e-učenje, a zatim na laboratorijskoj vježbi rješava zadatke i predaje rješenja koja se ocjenjuju. Student će rješavanjem zadanih zadataka na svakoj laboratorijskoj vježbi moći skupiti maksimalno 5 bodova, dakle ukupno na svih pet laboratorijskih vježbi maksimalno 25 bodova.

Projekt (dio)

Student samostalno ili u paru na praktičnom projektnom zadatku za konkretno zadani informacijski sustav određuje zaštitne funkcije informacijskog sustava te izrađuje ili konfigurira model autentifikacije i autorizacije korisnika za zadanu aplikaciju. Na taj način može steći maksimalno 20 bodova. Student mora ostvariti minimalno 50% (10 bodova) da bi izrađeni projektni zadatak smatrao uspješnim, čime ostvaruje uvjet za pristupanje završnom ispitu.

Završni ispit

Na teorijskom djelu student samostalno ili u paru izrađuje analizu rizika te argumentirano objašnjava postupke upravljanja razinom usluga, incidentima, problemima, zahtjevima i raspoloživošću (npr. izraditi tablicu odaziva s obzirom na vrstu problema i incidenta). Završni ispit se smatra položenim samo ako na njemu student postigne minimalno 50%-tni uspjeh (ispitni prag je 50% uspješno riješenih zadataka).

Ocjenjivanje

Kontinuiranim radom tijekom semestra na prethodno opisani način studenti/ce mogu ostvariti najviše 70 ocjenskih bodova, a da bi mogli pristupiti završnom ispitu moraju ostvarili 50% i više bodova (minimalno 35).

Završni ispit nosi udio od maksimalno 30 ocjenskih bodova, a smatra se položenim samo ako na njemu student/ica postigne minimalno 50%-ni uspjeh (ispitni prag je 50% uspješno riješenih zadataka).

Ukoliko je završni ispit prolazan, skupljeni bodovi će se pribrojati prethodnima i prema ukupnom rezultatu formirat će se pripadajuća ocjena. U suprotnom, student/ica ima pravo pristupa završnom ispitu još 2 puta (ukupno do 3 puta).

Konačna ocjena

Donosi se na osnovu zbroja svih bodova prikupljenih tijekom izvođenja nastave prema sljedećoj skali:

- A – 90%–100% (ekvivalent: izvrstan 5)
- B – 75%–89,9% (ekvivalent: vrlo dobar 4)
- C – 60%–74,9% (ekvivalent: dobar 3)
- D – 50%–59,9% (ekvivalent: dovoljan 2)
- F – 0%–49,9% (ekvivalent: nedovoljan 1)

Ispitni rokovi

Redoviti:

- 23. lipnja 2023.
- 07. srpnja 2023.

Izvanredni:

- 1. rujna 2023.
- 15. rujna 2023.

RASPORED NASTAVE – ljetni (IV.) semestar akademske godine 2022./2023.

Nastava će se na predmetu odvijati u zimskom semestru prema sljedećem rasporedu:

- predavanja: ponedjeljkom od 8:15 do 9:45 u O-028 i online
- vježbe: četvrtkom od 14:00 do 15:30 i od 16:00 do 17:30 u O-350

Tj.	Datum	Vrijeme	Prostor*	Tema	Nastava	Izvođač
1.	02. 3. 2023.	14:00–15:30 i 16:00–17:30	O-350	Uvod i motivacija. Hashiranje, kodiranje, šifriranje i zaporke (OpenSSL)	V1	Milan Petrović
1.	03.3. 2023.	12.:00–13:30	O-028	Sigurnosni rizici informacijskih sustava	P1	izv. prof. dr. sc. Božidar Kovačić
2.	09. 3. 2023.	14:00–15:30 i 16:00–17:30	O-350	Primjena kriptografije javnog ključa (OpenSSL)	V2	Milan Petrović
2.	10.3. 2023.	12.:00–13:30	O-028	Analiza i procjena rizika	P2	izv. prof. dr. sc. Božidar Kovačić
3.	16. 3. 2023.	14:00–15:30 i 16:00–17:30	online	Certifikat javnog ključa, certifikacijska tijela i sigurni poslužitelj (OpenSSL)	V3	Milan Petrović
3.	17.3. 2023.	12.:00–13:30	O-028	Prijetnje sigurnosti i vjerojatnost njihova nastanka	P3	izv. prof. dr. sc. Božidar Kovačić
4.	23. 3. 2023.	14:00–15:30 i 16:00–17:30	O-350	*Laboratorijska vježba 1:* Sigurna ljuska (OpenSSH)	V4	Milan Petrović
4.	24.3. 2023.	12.:00–13:30	O-028	Ranjivost informacijskih sustava	P4	izv. prof. dr. sc. Božidar Kovačić
5.	30. 3. 2023.	14:00–15:30 i 16:00–17:30	O-350	*Laboratorijska vježba 2:* Sigurnost virtualne privatne mreže (WireGuard)	V5	Milan Petrović
5.	31.4. 2023.	12.:00–13:30	O-028	Sigurnosni incidenti informacijskih sustava	P5	izv. prof. dr. sc. Božidar Kovačić
6.	06. 4. 2023.	14:00–15:30 i 16:00–17:30	O-350	*Laboratorijska vježba 3:* Web poslužitelj (HTTPie, Apache, ab)	V6	Milan Petrović
6.	07.4. 2023.	12.:00–13:30	O-028	Prepoznavanje znakova sigurnosnih incidenata	P6	izv. prof. dr. sc. Božidar Kovačić
7.	13. 4. 2023.	14:00–15:30 i 16:00–17:30	O-350	*Laboratorijska vježba 4:* Sigurni web poslužitelj (Apache, mod_ssl, OpenSSL)	V7	Milan Petrović
7.	14.4. 2023.	12.:00–13:30	O-028	Sigurnosni mehanizmi i kontrolni postupci	P7	izv. prof. dr. sc. Božidar Kovačić
8.	20. 4. 2023.	14:00–15:30 i 16:00–17:30	O-350	*Laboratorijska vježba 5:* Sigurnost baze podataka (MariaDB)	V8	Milan Petrović
8.	21. 4. 2023.	12.:00–13:30	O-028	Simetrična kriptografija	P9	izv. prof. dr. sc. Božidar Kovačić
9.	27. 4. 2023.	14:00–15:30 i 16:00–17:30	O-350	Simetrična kriptografija (Python)	V9	Milan Petrović
9.	28.4. 2023.	12.:00–13:30	O-028	**Kolokvij**	P8	izv. prof. dr. sc. Božidar Kovačić
10.	04. 5. 2022.	14:00–15:30 i 16:00–17:30	O-350	Asimetrična kriptografija (Python)	V10	Milan Petrović
10.	05. 5. 2023.	12:00–13:30	O-028	Asimetrična kriptografija	P10	izv. prof. dr. sc. Božidar Kovačić
11.	11. 5. 2022.	14:00–15:30 i 16:00–17:30	O-350	Autentifikacija i autentificirano šifriranje (Python)	V11	Milan Petrović

11.	12. 5. 2023.	12:00–13:30	O-028	Enkripcija i dekripcija podataka	P11	izv. prof. dr. sc. Božidar Kovačić
12.	18. 5. 2022.	14:00–15:30 i 16:00–17:30	O-350	Autentifikacija i sažeci poruka (Python)	V12	Milan Petrović
12.	19. 5. 2023.	12:00–13:30	online	Sigurnost transportnog sloja	P12	izv. prof. dr. sc. Božidar Kovačić
13.	25. 5. 2022.	14:00–15:30 i 16:00–17:30	O-350	Napadi na kriptografske algoritme (Python)	V13	Milan Petrović
13.	26. 5. 2023.	12:00–13:30	O-028	Upravljanje, poboljšanje i nadzor sustava informacijske sigurnosti. Mjerenje učinkovitosti kontrola	P13	izv. prof. dr. sc. Božidar Kovačić
14.	01. 6. 2022.	14:00–15:30 i 16:00–17:30	O-350	Sigurnost transportnog sloja (Python)	V14	Milan Petrović
14.	02. 6. 2023.	8:15–9:45	O-028	Upravljanje sigurnosnim rizicima. Metode za procjenu rizika	P14	izv. prof. dr. sc. Božidar Kovačić
15.	09. 6. 2023.	8:15–9:45	O-028	Upravljanje rizikom kao instrument unaprjeđivanja sigurnosti	P15	izv. prof. dr. sc. Božidar Kovačić

*upisati broj prostorije ili online

P – predavanja
V – vježbe