2024./2025.

Informacijski paket

Sveučilišni specijalistički studij Upravljanje sigurnošću i revizija informacijskih sustava

Informacijski paket skup je podataka ili informacija o visokom učilištu, studijskim programima i njihovim pojedinačnim sastavnicama (kolegiji, moduli i sl.) te o podršci studentima. Njegov je cilj olakšati razumijevanje i usporedbu studijskih programa te dati potpune informacije o profilima programa, kolegijima i sustavu studiranja. Informacijski paket izrađuje se na hrvatskome te u relevantnim dijelovima na engleskome jeziku i objavljuje na mrežnoj stranici sastavnice.

Informacijski paket sastoji se od tri dijela:

[1] Opće informacije o instituciji
[2] Informacije o studijskom programu
[3] Opis pojedinih kolegija

1. Opće informacije o instituciji:

a. naziv i adresa

Naziv: Sveučilište u Zagrebu Fakultet organizacije i informatike (SUZG FOI)

Adresa: Pavlinska 2, 42000 Varaždin

Tel: 042/390800

Fax: 042/213413

E-mail: ured-dekana@foi.hr

URL: http://www.foi.unizg.hr

b. opći opis institucije (uključujući vrstu i status)

Sveučilište u Zagrebu Fakultet organizacije i informatike (SUZG FOI) jedno je od najvažnijih visokih učilišta u Hrvatskoj u području informacijskih znanosti i središnje mjesto razvoja informatičke struke u Hrvatskoj, a u zadnjih 15 godina SUZG FOI se etablira kao značajno središte za razvoj studijskog programa u području ekonomije. Korijeni SUZG FOI-ja sežu u 1962. godinu, kada je osnovana Viša ekonomska škola, na čijim temeljima je 1974. godine osnovan Fakultet organizacije i informatike. SUZG FOI je sastavnica Sveučilišta u Zagrebu koja djeluje u području društvenih znanosti, u polju informacijskih znanosti (5.04), zatim u polju ekonomije (5.01), te manjim dijelom u drugim znanstvenim područjima i poljima, poput računarstva, matematike i obrazovnih znanosti čime se potvrđuje interdisciplinarnost djelovanja SUZG FOI.

c. kalendar nastave i ispita

Nastava na sveučilišnom specijalističkom studiju USRIS izvodi se:

2024-2025 Raspored nastave 1. semestar

OŽUJAK

P	U	S	Č	P	S	N
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

TRAVANJ

P	U	S	Č	P	S	N
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

SVIBANJ

P	U	S	Č	P	S	N
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

LIPANJ

P	U	S	Č	P	S	N
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

SRPANJ

P	U	S	Č	P	S	N
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Popis predmeta

Obavezni predmet	Ukupno sati
Upravljanje informatičkom sigurnošću	20
Upravljanje rizicima informacijske sigurnosti	20
Revizija i kontrola IS-a	25
Upravljanje kontinuitetom poslovanja	25
Upravljanje incidentima i računalna forenzika	20

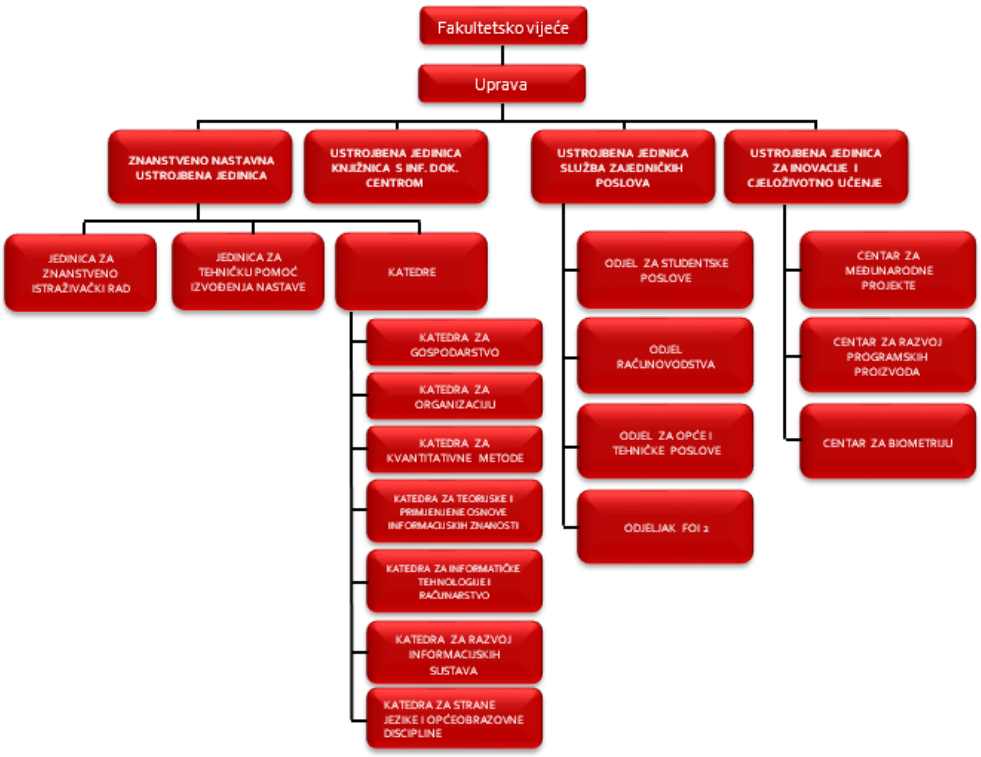
- sinkroni prijenos iz dvorane prilikom kontaktne nastave
- nastava petak od 16, subota od 9 sati

d. popis djelatnika na SZFOI-ju

Djelatnik	Radno mjesto
Katedra za gospodarstvo	
Bubanić Marijana	Viši asistent
Detelj Kristina	Izvanredni profesor
Dobrinić Damir	Redoviti profesor u trajnom izboru
Dvorski Lacković Ivana	Viši asistent
Đunđek Ivana	Docent
Gregurec Iva	Šef katedre/Izvanredni profesor
Keglević Kozjak Suzana	Docent
Klačmer Čalopa Marina	Redoviti profesor
Kocijan Ivona	Asistent
Konecki Irena	Izvanredni profesor
Korent Dina	Docent
Kovšca Vladimir	Redoviti profesor
Kuštelega Magdalena	Asistent
Lacković Vincek Zrinka	Izvanredni profesor
Šestanj Perić Tanja	Viši predavač
Šmaguc Tamara	Docent
Vuković Ksenija	Redoviti profesor u trajnom izboru
Katedra za informatičke tehnologije i računarstvo	
Balaban Igor	Redoviti profesor
Grd Petra	Izvanredni profesor
Ivković Nikola	Izvanredni profesor
Magdalenić Ivan	Redoviti profesor
Markić Danijela	Asistent
Matus Marko	Asistent
Mihaljević Ivan	Predavač
Milić Luka	Viši asistent
Milošević Roko	Asistent
Popović Elvis	Asistent
Tomičić Igor	Šef katedre/Izvanredni profesor
Tuličić Domagoj	Asistent
Zlatović Miran	Viši predavač
Katedra za kvantitativne metode	
Bosak Mihaela	Predavač
Buhin Pandur Maja	Predavač
Divjak Blaženka	Šef katedre/Redoviti profesor u trajnom izboru
Dobša Jasminka	Redoviti profesor u trajnom izboru
Erjavec Zlatko	Redoviti profesor
Gusić Munđar Jelena	Predavač
Horvat Damir	Viši predavač
Jakuš Marija	Viši predavač
Maretić Marcel	Docent
Mavrek Iva	Asistent

Perši Nenad	Viši predavač
Svetec Barbi	Asistent
Žajdela Hrustek Nikolina	Izvanredni profesor
Žugec Bojan	Docent
Žugec Petra	Docent
Katedra za organizaciju	
Begičević Ređep Nina	Redoviti profesor
Bubaš Goran	Redoviti profesor u trajnom izboru
Devčić Antonela	Viši asistent
Dreven Nikolina	Viši asistent
Fabac Robert	Šef katedre/Redoviti profesor u trajnom izboru
Hrustek Larisa	Asistent
Jagačić Tena	Asistent
Kadoić Nikola	Docent
Kokot Karolina	Viši asistent
Kutnjak Ana	Asistent
Malbašić Ivan	Izvanredni profesor
Pihir Igor	Izvanredni profesor
Pikl Lorena	Asistent
Šlibar Barbara	Asistent
Tomičić Furjan Martina	Prodekan
Vidaček-Hainš Violeta	Redoviti profesor
Katedra za razvoj informacijskih sustava	
Andročec Darko	Izvanredni profesor
Draganić Melita	Redoviti profesor
Kirinić Valentina	Redoviti profesor
Križanić Snježana	Asistent
Kuštelega Marija	Asistent
Mekovec Renata	Redoviti profesor
Mihaljević Matej	Asistent
Mijač Marko	Docent
Oreški Dijana	Izvanredni profesor
Pažur Aničić Katarina	Izvanredni profesor
Peras Dijana	Asistent
Picek Ruben	Redoviti profesor
Plantak Vukovac Dijana	Izvanredni profesor
Pokos Lukinec Marija	Asistent
Posarić Lovro	Asistent
Shareef Ahmed	Asistent
Stapić Zlatko	Prodekan
Strahonja Vjeran	Redoviti profesor
Šajn Matija	Asistent
Tomičić-Pupek Katarina	Šef katedre/Redoviti profesor
Višnjić Dunja	Asistent
Vrček Neven	Redoviti profesor u trajnom izboru

Katedra za strane jezike i općeobrazovne discipline	
Hajdin Goran	Šef katedre/Izvanredni profesor
Kovačić Andreja	Viši predavač
Vučić Damir	Viši predavač
Katedra za teorijske i primijenjene osnove informacijskih znanosti	
Cerjan Maja	Asistent
Kaniški Matija	Predavač
Kermek Dragutin	Redoviti profesor u trajnom izboru
Konecki Mario	Izvanredni profesor
Konecki Mladen	Docent
Kudelić Robert	Izvanredni profesor
Lovrenčić Alen	Redoviti profesor u trajnom izboru
Lovrenčić Sandra	Šef katedre/Redoviti profesor u trajnom izboru
Maček Marija	Asistent
Novak Matija	Docent
Novaković Miljenko	Predavač
Peharda Tomislav	Asistent
Rabuzin Kornelije	Redoviti profesor u trajnom izboru
Radošević Danijel	Redoviti profesor u trajnom izboru
Schatten Markus	Redoviti profesor
Sekovanić Vlatka	Predavač
Vlahek Dino	Docent



Slika 1: Prikaz organizacijske strukture SUZG FOI-ja

e. popis studijskih programa

Na prijediplomskoj razini, SUZG FOI izvodi jedan sveučilišni studijski program u području informacijskih znanosti – **Informacijski i poslovni sustavi (IPS)**, koji obuhvaća četiri usmjerenja: Razvoj programskih sustava, Umjetna inteligencija u poslovanju, Umreženi sustavi i računalne igre te Analiza i dizajn poslovnih sustava. Nakon završetka studija dodjeljuje se titula **sveučilišni prvostupnik/prvostupnica informatike**. U području ekonomije na prijediplomskoj razini, SUZG FOI izvodi sveučilišni studijski program **Ekonomika poduzetništva (EP)**. Nakon završetka studija dodjeljuje se titula **sveučilišni prvostupnik/prvostupnica ekonomije**.

Na diplomskoj razini, SUZG FOI izvodi **četiri sveučilišna studijska programa u području informacijskih znanosti** – **Informacijsko i programsko inženjerstvo (IPI), Organizacija poslovnih sustava (OPS), Baze podataka i baze znanja (BPBZ) te Informatika u obrazovanju (IuO)**, a studentima se nakon završetka studija dodjeljuje titula **sveučilišni magistar/magistra informatike ili informatike u obrazovanju**. Na diplomskoj razini se izvodi i jedan sveučilišni studijski program u području ekonomije – **Ekonomika poduzetništva (EP)**, a studentima se nakon završetka studija dodjeljuje titula **sveučilišni magistar/magistra ekonomije**.

Uz sveučilišne studije, SUZG FOI izvodi i jedan stručni prijediplomski studij u području informacijskih znanosti – **Informacijske tehnologije i digitalizacija poslovanja (ITDP)**. Nakon završetka studija dodjeljuje se titula **prvostupnik/prvostupnica primijenjene informatike**.

Na poslijediplomskoj razini, SUZG FOI je **nositelj doktorskog studija Informacijske znanosti (IZ)**, na kojem se studentima nakon završetka studija dodjeljuje **titula doktor/doktorica znanosti iz znanstvenog područja društvenih znanosti, znanstveno polje informacijske znanosti**. SUZG FOI je sunositelj **doktorskog studija Upravljanje digitalnim inovacijama (UDI)** s Ekonomskim fakultetom Sveučilišta u Zagrebu, a studentima se nakon završetka studija dodjeljuje **titula doktor/doktorica znanosti iz područja društvenih znanosti, polje ekonomija, grana poslovna informatika.**

SUZG FOI samostalno izvodi **dva specijalistička studija** (**Menadžment poslovnih sustava** (MPS, u području ekonomije), **Upravljanje sigurnošću i revizijom informacijskih sustava** (USiRIS, u području informacijskih znanosti) te sveučilišni specijalistički studij **E-učenje u obrazovanju i poslovanju** (EUOP, u području informacijskih znanosti) u suradnji sa Filozofskim fakultetom Zagreb i CARNET-om. Studentima se nakon završetka specijalističkih studija dodjeljuje titula specijalist/ica upravljanja sigurnošću i revizije informacijskih sustava, specijalist/a e-učenja ili sveučilišni/a specijalist/a menadžmenta poslovnih sustava.

Osim toga, SUZG FOI sudjeluje kao institucionalni sunositelj na sveučilišnim studijama, Hrvatskog vojnog učilišta "Dr. Franjo Tuđman" u Zagrebu.

		Naziv studijskog programa	ECTS bodovi	Mjesto izvođenja	Izvodi se od
PRIJEDIPLOMSKI	SVEUČILIŠNI	Ekonomika poduzetništva	180	Varaždin	2007.
		Informacijski i poslovni sustavi Usmjerenje: Razvoj programskih sustava, Umjetna inteligencija u poslovanju, Umreženi sustavi i računalne igre te Analiza i dizajn poslovnih sustava	180	Varaždin	2005.
	STRUČNI	Informacijske tehnologije i digitalizacija poslovanja Usmjerenje: Razvoj aplikacija, Informatička podrška poslovanju	180	Zagreb	2023.
		Informacijske tehnologije i digitalizacija poslovanja	180	Sisak	2022.
		Informacijske tehnologije i digitalizacija poslovanja	180	Varaždin	2022.
DIPLOMSKI	SVEUČILIŠNI	Baze podataka i baze znanja	120	Varaždin	2005.
		Ekonomika poduzetništva	120	Varaždin	2017.
		Informacijsko i programsko inženjerstvo	120	Varaždin	2005.
		Informatika u obrazovanju	120	Varaždin	2006.
		Organizacija poslovnih sustava	120	Varaždin	2005.
POSLIJEDIPLOMSKI	SPECIJALISTIČKI	E-učenje u obrazovanju i poslovanju	90	Varaždin	2021.
		Menadžment poslovnih sustava	90	Varaždin	2007.
		Upravljanje sigurnošću i revizija informacijskih sustava	90	Varaždin	2007.
	DOKTORSKI	Informacijske znanosti	180	Varaždin	2006.
		Upravljanje digitalnim inovacijama (u suradnji sa EFZG)	180	Varaždin	2024.

Tablica 1: Pregled studijskih programa

SUZG FOI je također prijavio na Sveučilištu u Zagrebu programe cjeloživotnog obrazovanja (Program Pedagoško-psihološko-didaktičko-metodičko obrazovanje, Program izobrazbe iz javne nabave, radionice za mentore na doktorskom studiju) koji se organiziraju radi stjecanja znanja, vještina i kompetencija za osobne, društvene i profesionalne potrebe te potrebe tržišta rada.

Ujedno, SUZG FOI se sustavno bavi prilagodbom svojih studijskih programa i poslovnih procesa prema međunarodnim standardima i smjernicama organizacija kao što su EFMD (engl. European Foundation for Management Development) i ASIIN (eng. Accreditation Agency for Degree Programs in Engineering, Informatics/Computer Science, Natural Sciences and Mathematics). EFMD je u 2024. godini akreditirao sveučilišni diplomski studijski program Ekonomika poduzetništva, čime je potvrđena visoka kvaliteta obrazovanja usklađena s najvišim europskim standardima. SUZG FOI je početkom 2025. godine započeo proces ASIIN akreditacije sveučilišnog prijediplomskog studijskog programa Informacijski i poslovni sustavi.

2. Informacije o studijskom programu

A) Općeniti opis:

a. postupak i uvjeti prijave

Na studij Upravljanje sigurnošću i revizija informacijskih sustav (USRIS) mogu se izravno upisati pristupnici koji su završili odgovarajući sveučilišni diplomski studij iz područja društvenih, tehničkih ili prirodnih znanosti u trajanju od osam semestra i imaju 300 ECTS bodova s prosječnom ocjenom 3,5 i višom.

Sveučilišni specijalistički studij može upisati osoba koja je završila odgovarajući sveučilišni diplomski studij ili sveučilišni integrirani prijediplomski i diplomski studij. Iznimno, sveučilišni specijalistički studij može upisati i osoba koja je završila stručni diplomski studij uz polaganje razlikovnih ispita koje određuje Fakultet, odnosno uz najmanje 5 godina radnog staža u području izvođenja studija. Student državljanin države članice Europske unije ima ista prava kao i student hrvatski državljanin. Državljani ostalih zemalja upisuju se na studij pod jednakim uvjetima kao i hrvatski državljani uz obvezu plaćanja studija u skladu sa Zakonom i općim aktom Sveučilišta i Fakulteta.
Odgovarajući sveučilišni diplomski studij je svaki studij na kome se izučavaju sadržaji iz znanstvenih polja informacijskih i računalskih znanosti.

Tekst natječaja za upis studenata na sveučilišne specijalističke studije u akademskoj godini 2024./2025. objavljen je na linku.

Prijavi na natječaj za upis na specijalističke studije treba priložiti:

- ovjerene prijepise (preslike) diplome i svjedodžbe dodiplomskog studija
- ovjereni prijepis ocjena dodiplomskog studija iz svih predmeta (samo pristupnici koji nisu završili dodiplomski studij na Sveučilištu u Zagrebu Fakultetu organizacije i informatike)
- dokaz o poznavanju jednog svjetskog jezika
- životopis
- rodni list i
- dokaz o državljanstvu.

Izbor između pristupnika obavlja se razredbenim postupkom kojeg provodi Odbor odgovarajućeg sveučilišnog specijalističkog studija. Pristupnici koji su završili srodni diplomski ili integrirani studij, a nemaju potrebne ulazne kompetencije za upis odabranog sveučilišnog specijalističkog studija, iste mogu steći upisom razlikovnih kolegija.

b. trajanje programa studija: 3 semestra

c. voditelj studija - voditeljica studija je: prof. dr. sc. Renata Mekovec

d. razina kvalifikacije prema Hrvatskom i Europskom kvalifikacijskom okviru: 7.2.

e. ishodi učenja na razini studijskog programa

Ishodi učenja programa

1. Analizirati resurse informacijskog sustava s aspekta njihove ranjivosti i sigurnosnih nedostataka.
2. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike.
3. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti.

4. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti.
5. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
6. Definirati, osmisliti i primijeniti strategiju uspostave sustava informacijske sigurnosti.
7. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava,zaposlenici, klijenti, institucije državne uprave).
8. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture.
9. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/informacijskom sustavu.
10. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti.
11. Procijeniti utjecaj sigurnosne strategije, sigurnosnih politika, zakonskog okvira, primijenjenih sigurnosnih rješenja na poslovni/informacijski sustav, te pripadajući sustav informacijske sigurnosti.
12. Uspostaviti i primijeniti planove i procedure za osiguranje informacijske imovine, uključujući i planove oporavka, u skladu s međunarodnim normama, zakonskim aktima i iskustvima dobre prakse.
13. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava
14. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti.
15. Uspostaviti i provoditi učinkovit trening za podizanje znanja i svijesti o informacijskoj sigurnosti s ciljem provođenja usvojenih sigurnosnih politika i procedura.

f. način studiranja (u punoj ili prilagođenoj nastavnoj satnici) – u skladu s izvedbenim programom

g. informacije o obliku diplome i dopunske isprave o studiju - Nakon završetka studija izdaje se diploma o završenom sveučilišnom specijalističkom studiju. Uz diplomu izdaje se dopunska isprava o studiju. Diploma i dopunska isprava o studiju javne su isprave kojima se potvrđuje da je student završio studij i stekao pravo na akademski naziv u skladu sa Zakonom. Na diplomi se upisuje broj bodova prema ECTS-u studija, a na dopunskoj ispravi o studiju broj stečenih bodova prema ECTS-u. Oblik i sadržaj javnih isprava utvrđuju se pravilnikom koji uređuje oblik i sadržaj svjedodžbe, diplome i dopunske isprave o studiju.

h. kvalifikacija koja se stječe završetkom studija - Izradom i obranom specijalističkog rada polaznik stječe 90 ECTS bodova. Na temelju toga dobiva akademski naziv **specijalist/ica upravljanja sigurnošću i revizije informacijskih sustava, spec. inf.**

i. moguć pristup daljnjem studiranju - Nakon završenog specijalističkog studija, moguće je upisati sveučilišni doktorski studij prema kriterijima upisa.

j. struktura studijskog programa, uz bodove prema Europskom sustavu stjecanja i prijenosa bodova (dalje: ECTS)

Nastava se izvodi u skladu s odredbama izvedbenog plana studija. Upisom pojedinoga kolegija, obveznog ili izbornog, student preuzima sve obveze predviđene planom i programom toga kolegija. Ostvarivanje ishoda učenja studenta provjerava se i vrednuje tijekom nastave (kolokviji, praktične zadaće, projekti, artefakti i sl.), a konačna se ocjena određuje na ispitu.

Studijski program izvodi se u tri semestra. U prvom i drugom semestru izvodi se nastava obaveznih i izbornih kolegija. U trećem semestru izrađuje se završni rad.

Sve o kolegijima, ciljevima, ishodima učenja te te sadržaju predmeta dostupne su na mrežnim stranicama studija. Informacije o izvođačima i njihovim kontaktima dostupne su u aplikaciji nastava.foi.hr.

Suradnja s (ISC)2 i stručni certifikati – studij USRIS izrađen je u suradnji sa najvećom svjetskom organizacijom lidera u informacijskoj sigurnosti – (ISC)² i renomiranim stručnjacima, te program studija uključuje kompletnu pripremu polaznika za polaganje globalno najtraženijeg stručnog certifikata CISSP (dostupan besplatan upis u ISC2 Adaptive Online Self-Paced Training). Također, program svakog predmeta na ovom studiju izrađen je u skladu s potrebama tržišta za specifičnim znanjima iz područja informacijske sigurnosti i predstavlja odličnu osnovu za polaganje brojnih priznatih stručnih certifikata.

PREDMET	STATUS PREDMETA	NOSITELJI	SURADNICI	Broj ECTS
Upravljanje rizicima u informacijskoj sigurnosti	Obavezan	Ivan Magdalenić	Davor Maček	6
Upravljanje informacijskom sigurnošću	Obavezan	Željko Hutinski Mario Spremić	Renata Mekovec	6
Revizija i kontrola informacijskih sustava	Obavezan	Melita Kozina Mario Žgela	Valentina Kirinić	6
Upravljanje incidentima i računalna forenzika	Obavezan	Igor Tomičić Petra Grd		6
Upravljanje kontinuitetom poslovanja	Obavezan	Mario Žgela Valentina Kirinić	Biljana Cerin	6
Specijalistički rad	Obavezan			30
Sigurnost umreženih računalnih sustava	Izborni	Ivan Magdalenić Nikola Ivković Muhamed Turkanović	Luka Milić	5
Sigurnost baza podataka	Izborni	Markus Schatten	Bogdan Okreša Đurić	5
Primijenjena kriptografija i sustavi sigurnosti	Izborni	Ivan Magdalenić Marin Golub Marcel Maretić	Marko Hölbl	5
Sustavi fizičke i logičke kontrole pristupa	Izborni	Petra Grd		5
Sigurnost web i poslužiteljskih aplikacija	Izborni	Dragutin Kermek Marko Hölbl Muhamed Turkanović	Matija Novak	5
Zaštita osobnih podataka	Izborni	Renata Mekovec	Ioanna Danidou	5

		Christiana Markau		
Sigurnosna pohrana, arhiviranje i repozitoriji podataka	Izborni	Markus Schatten	Dr.sc. Bogdan Okreša Đurić	5
Sigurnost operacijskih sustava	Izborni	Ivan Magdalenić Marin Golub		5
Testiranje sustava sigurnosti i etičko hakiranje	Izborni	Igor Tomičić Nikola Ivković		5
Sigurnost Interneta stvari	Izborni	Boris Tomaš Neven Vrček	Luka Milić	5
Socijalni inženjering	Izborni	Igor Tomičić		5
Dizajn sigurnih programskih proizvoda	Izborni	Zlatko Stapić Neven Vrček		5
Sigurnost digitalnog poslovanja	Izborni	Ne izvodi se u akademskoj godini 2024./25.		
Informacijsko ratovanje i računalni kriminal	Izborni	Ne izvodi se u akademskoj godini 2024./25.		

k. informacije o završetku studija (obrana završnog ili diplomskog rada; završni ili diplomski ispit, ako je primjenjivo) i pravila ispitivanja i ocjenjivanja - Studij završava polaganjem svih ispita, ispunjenjem drugih studijskih obveza te izradom i obranom specijalističkog rada. Za završetak studija student treba ostvariti najmanje 90 bodova prema ECTS-u pri čemu mora položiti sve obvezne kolegije studija te odabrane izborne kolegije. Postupak prihvaćanja teme sveučilišnog specijalističkog rada student može pokrenuti nakon što je stekao barem 40 bodova prema ECTS-u. Student kojem je prihvaćena tema specijalističkog rada može pokrenuti postupak ocjene specijalističkog rada tek nakon što je položio sve obvezne kolegije i stekao barem 60 bodova prema ECTS-u.

B) Opis pojedinih kolegija:

Tablica 2. A Opis kolegija

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Zlatko Stapić Neven Vrček	1.6. Godina studija	1
1.2. Naziv predmeta	**Dizajn sigurnih programskih proizvoda**	1.7. Broj bodova po ECTS sustavu	4
1.3. Suradnici		1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	10+10+10
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni predmet	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Cilj predmeta *Dizajn sigurnih programskih proizvoda* je upoznati studente sa ključnim aspektima dizajna arhitekture i strukture sigurnog softvera i mobilnih programskih proizvoda te upravljanjem sigurnošću u procesu razvoja. Predmet uključuje prikaz najboljih praksi inženjerstva sigurnih sustava (softvera, mobilnih aplikacija) kroz sve faze razvoja programskog proizvoda s posebnim naglaskom na fazu dizajna. Kroz kurikulum su pokriveni aspekti sigurnosti koje odnose na sigurnost pojedinih podsustava, ali i njihove integracije i komunikacije te sustava u cjelini.		
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata procesa razvoja programskih proizvoda i informacijskih sustava te implementacije mjera informacijske sigurnosti.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/informacijskom sustavu. 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti. 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske 4. sigurnosti. 5. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 6. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 7. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.		
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Analizirati i prepoznati potencijalne prijetnje sigurnosti programskog proizvoda 2. Ugraditi i primijeniti aspekte razvoja informacijske sigurnosti u procesu razvoja programskih proizvoda 3. Izgraditi arhitekturu i dizajn programskog proizvoda s ugrađenim elementima sigurnosti 4. Prepoznati, razumjeti i ukloniti sigurnosne prijetnje pri dizajnu i razvoju aplikacija za mobilne platforme 5. Definirati proces testiranja i analize sigurnosti mobilnih programskih proizvoda		

5.1. Sadržaj predmeta	1. Sigurnost programskih proizvoda Aspekti sigurnosti programskih proizvoda. Aspekti sigurnosti u praksama programskog inženjerstva. Proaktivan pristup sigurnom razvoju programskih proizvoda. Životni ciklus razvoja sigurnih programskih proizvoda. Modeli zrelosti sigurnosti softvera. Aplikacijska sigurnost. Alati aplikacijske sigurnosti. Ranjivosti softvera. 2. Integracija sigurnosti u životni ciklus proizvoda Osnove DevSecOps principa: definiranje ovlasti i odgovornosti u postupku razvoja, puštanja u pogon, održavanja i povlačenja aplikacija i određivanje ovlasti za pristup produkcijskim podacima. Organizacija sigurnog razvoja programskih proizvoda: recenziranje koda, programiranje u paru, automatizirano testiranje prije implementacije, norme za sigurni razvoj i testiranje, norme za verifikaciju razine sigurnosti. 3. Arhitektura sigurnih proizvoda Koncepti sigurnosti u dizajnu arhitekture programskih i mobilnih proizvoda. Identifikacija sigurnosnih rizika i ranjivosti softvera na arhitekturnoj razini. Sigurne aplikacijske arhitekture. Sigurne distribuirane arhitekture. Arhitektura otvorenog softvera. Najbolje prakse u dizajnu arhitekture programskih proizvoda i mobilnih aplikacija. 4. Principi dizajna sigurnih proizvoda Koncepti dizajna sigurnih sustava: slojevi, apstrakcija, domene sigurnosti, otvoreni i zatvoreni sustavi. Enkapsulacija. Validacija podataka. Validacija ulaznih podataka. Enkripcija izlaznih podataka. Upravljanje iznimkama i logovima. Dobre prakse dizajna sigurnih programskih proizvoda i mobilnih aplikacija. 5. Dizajn i razvoj sigurnih mobilnih aplikacija Specifičnosti razvoja mobilnih programskih proizvoda. Sigurnosni aspekti u razvoju mobilnih aplikacija. Sigurnosni aspekti mobilnih aplikacijskih arhitektura i upravljanja podacima. Prakse dizajna i razvoja sigurnih mobilnih aplikacija. 6. Dizajn i razvoj sigurnih više-platformskih sustava Sigurnost više-platformskih sustava. Sigurnosni aspekti u razvoju više-platformskih aplikacija. Sigurnosni aspekti više-platformskih aplikacijskih arhitektura i upravljanja podacima. Prakse dizajna i razvoja sigurnih više-platformskih sustava. 7. Sigurnosni aspekti aplikacija za Android Android operacijski sustav. Osnovni koncepti razvoja android aplikacija. Arhitektura android aplikacija. Aktivnosti, fragmenti, pozadinski servisi. Sigurnosni rizici android aplikacija. Prakse zaštite sigurnosti kod razvoja za Android. Biblioteke trećih strana. 8. Sigurnosni aspekti aplikacija za iOS Operacijski sustav iOS. Osnovni koncepti razvoja aplikacija za iOS. Arhitektura iOS aplikacija. Core OS, Core Services Layer, Media Layer, Cocoa Touch Layer. Sigurnosni rizici iOS aplikacija. Prakse zaštite sigurnosti kod razvoja za iOS. Biblioteke trećih strana. 9. Integracija sigurnih sustava

	Sigurnosni aspekti točaka integracije podsustava u cjelovito rješenje. Integracijski koncepti. Tipovi integracije. Analiza i uklanjanje sigurnosnih rizika. 10. Testiranje i analiza sigurnosti Priprema podataka za testiranje: generiranje podataka, anonimizacija, maskiranje. Prakse osiguranje kvalitete. Automatizirano testiranje. Kontinuirana sigurnost. Sigurnost vođena testiranjem. Testiranje u kontekstu DevSecOps-a.

2.6. Sadržaj predmeta			2.7. Komentari:
	☒ predavanja ☒ seminari i radionice ☒ vježbe ☐ on line u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☐ mentorski rad ☐ (ostalo upisati)	

2.8. Obveze studenata	
	Studenti preuzimaju i odrađuju samostalni projekt dizajna arhitekture ili strukture programskog proizvoda ili mobilne aplikacije iz odabrane domene tehničke ili organizacijske specijalizacije. Poželjno je da je domena problemskog zadatka iz područja rada tj. radnih obaveza kandidata. U terminu seminara kandidati prezentiraju i brane predloženo rješenje. U terminu usmenog ispita kandidat ima klasični usmeni ispit, a kod konačne ocjene se u obzir uzima i obranjeni projektni rad.

2.9. Praćenje rada studenata								
Pohađanje nastave	DA	NE	Projekt	DA		Pismeni ispit	DA	
Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
Esej			Referat			(ostalo upisati)		
Kolokvij			Seminarski rad	DA		(ostalo upisati)		
			Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)	4	

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Ransom James, Misra Anmol: Core Software Security: Security at the source. CRC Press, 2014 ili novije izdanje.		

2.11. Dopunska literatura (navesti naslov)	
	1. Rerup Neil, Aslaner Milad: Hands-on Cypersecurity for Architects, Packt publishing 2018. ili novije izdanje.

	2. Helfrich James: Security for Software Engineers. CRC Press, 2019 ili novije izdanje. 3. Deogun Daniel, Johnson Den Bergh, Sawanso Daniel: Secure by Design. Manning Publications 2019. ili novije izdanje. 4. Vehnet Julien: Securing DevOps – Security in the Cloud. Manning Publications 2018. ili novije izdanje. 5. Axelrod C. Warren: Engineering Safe and Secure Software Systems. Artech Hose, 2013 ili novije izdanje. 6. Dwivedi Himanshu, Clark Chris, Thiel David: Mobile Application Security: Protecting Mobile Devices and their Applications. McGraw Hill Professional 2010 ili novije izdanje. 7. Chell Dominic, Erasmus Tyrone, Colley Shaun, Whitehouse Ollie: The Mobile Application Hacker's Handbook, Wiley 2015 ili novije izdanje. 8. Elenkov Nikolay: Android Security Internals: An In-Depth Guide to Android's Security Architecture, No Starch Press 2014. ili novije izdanje. 9. Thiel David: iOS Application Security: The Definitive Guide for Hackers and Developers. No Starch Press, 2016 ili novije izdanje 10. Mahfuz Sayed Abu: Software Quality Assurance – Integrating Testing, Security and Audit. CRC Press 2016 ili novije izdanje. 11. Merkow Mark S., Raghavan Lakshmikanth: Secure and Resilient Software Development, CRC Press, 2010 ili novije izdanje. 12. Viega John, McGraw Gery: Building Secure Software: How to avoid Security Problems the Right Way. Addison-Wesley 2002 ili novije izdanje.

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Renata Mekovec Christiana Markou	1.6. Godina studija	1
1.2. Naziv predmeta	**Privatnost i osobni podaci**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici	Ioanna Danidou	1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20+0+10
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Upoznati studente s važnošću zaštite privatnosti pojedinca Upoznati studente s različitim zakonodavnim okvirom i praksama vezanim uz zaštitu privatnosti pojedinca prilikom njegovog korištenja različitih tehnoloških dostignuća Osposobiti studente da izrade, pročitaju, razumiju i procijene politiku privatnosti, obavijest o prikupljanju, obradi i korištenju osobnih podataka i privolu za prikupljanje, obradu i korištenje osobnih podataka		

	Osposobiti studente da diskutiraju o implikacijama vezanim uz privatnost sa zakonodavcem, poslodavcem i inženjerima koji sudjeluju u razvoju različitih usluga/proizvoda podržanim upotrebom IT
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata zaštite osobnih podataka.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti. 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti 4. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 5. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Kritički prosuđivati različite vrste osobnih podataka pojedinca koje smije/ne smije prikupljati, obrađivati, brisati, editirati, arhivirati i dijeliti druga fizička ili pravna osoba 2. Valorizirati važnost zaštite osobnih podataka od strane pojedinca, različitih poslovnih subjekata i vladinih institucija 3. Kritički prosuđivati nacionalne i međunarodne propise koji uređuju zaštitu osobnih podataka kao i primjere praksi vezanih uz zaštitu osobnih podataka 4. Preporučiti osnovne elemente zbirke osobnih podataka te zadatke i odgovornosti voditelja zbirke osobnih podataka i službenika za zaštitu osobnih podataka 5. Izraditi politiku zaštite osobnih podataka za konkretnu organizaciju 6. Analizirati rizike vezane uz zaštitu osobnih podataka za konkretnu organizaciju i izraditi plan zaštite osobnih podataka 7. Kreirati obrazac privole, izjavu o čuvanju tajnosti podataka i obavijest o prikupljanju, obradi i korištenju podataka 8. Analizirati moguće povrede privatnosti te identificirati mogućnosti zaštite osobnih podataka pri primjeni različitih tehnoloških dostignuća 9. Prepoznati različite načine povrede privatnosti te ih proaktivno sprečavati kroz individualno djelovanje Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: 1. IAPP CIPP/E Certified Information Privacy Professional/Europe 2. ISACA CDPSE Certified Data Privacy Solutions Engineer
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	OSNOVE PRIVATNOSTI - Privatnost kao koncept. Privatnost kao pravo. Definicije privatnosti. Kontrola nad osobnim podacima. Funkcije privatnosti. Vrste privatnosti. Vrste povrede privatnosti. PRINCIPI ZAŠTITE PRIVATNOSTI - Ispravno ophođenje s informacijama. Principi ispravnog ophođenja s informacijama. Kodeks ispravnog ophođenja s informacijama. Principi vezani uz zaštitu podataka. Okvir privatnosti.

	ZAKONODAVNI OKVIR - Nacionalni zakonodavni okvir. Međunarodni zakonodavni okvir. Primjeri samoregulacije u određenim djelatnostima. Primjeri praksi vezanih uz zaštitu podataka i privatnosti pojedinca. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA - Chief Privacy officer, Data protection officer. Zadaci i odgovornosti službenika za zaštitu osobnih podataka. Zadaci i odgovornosti voditelja zbirki osobnih podataka. OSOBNI PODACI - Prikupljanje, obrada, diseminacija, dijeljenje, i arhiviranje osobnih podataka. Izravna i neizravna identifikacija. Uvid u osobne podatke. Zbirke osobnih podataka. Iznošenje osobnih podataka u inozemstvo. POLITIKA PRIVATNOSTI - Politika privatnosti. Izjava o tajnosti podataka. Obavijest o prikupljanju, obradi i korištenju osobnih podataka. Privola za prikupljanje, obradu i korištenje osobnih podataka. Opt-in i Opt-out. ZAŠTITA PRIVATNOSTI NA RADNOM MJESTU - Potrebni podaci za postupak zapošljavanja. Pitanja povezana s obradom podataka za vrijeme radnog odnosa. Tehnike nadzora na radnom mjestu. Zaštita podataka i prestanak radnog odnosa. Nadzor od strane vladinih institucija. Zaštita privatnosti u medicini. ZABRINUTOSTI VEZANE UZ ZAŠTITU PRIVATNOSTI - Internet nadzor i web praćenje. "Do not track" standard. Biometrijsko prepoznavanje pojedinca. Identificiranje i praćenje lokacije. Privatnost i društvene mreže. Privatnost i pametni telefoni. Privatnost i pametna okolina. Privatnost i big data fenomen. Privatnost i sustavi nadzora. Procjena legitimnog interesa. UPRAVLJANJE PRIVATNOŠĆU - Načini zaštite privatnosti. Zaštita privatnosti zakonom. Zaštita privatnosti tehnologijom. Privacy engeenering. Privacy by design. Privacy impact assessment - PIA. Okvir upravljanja privatnošću. Seminari - Na seminarima se studenti šire i dublje upoznavanju s materijom obrađenom na predavanjima.
2.6. Vrste izvođenja nastave:	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ *on line* u cijelosti ☐ mješovito e-učenje ☐ terenska nastava ☐ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)
2.7. Komentari:	
2.8. Obveze studenata	Vježbe: Napraviti procjenu legitimnog interesa i procjenu učinka na zaštitu podataka na odgovarajućim primjerima aktivnosti obrada osobnih podataka. Odabir ispravne metode zaštite podataka u pojedinim slučajevima (anonimizacija, pseudonimizacija, enkripcija). Određivanje sigurnosnih zahtjeva za izvršitelje obrade.

2.9. Praćenje rada studenata									
	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		
	Kolokvij			Seminarski rad			(ostalo upisati)		
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**	

2.10. Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	**Naslov**	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**

	Treder, M. The Chief Data Officer Management Handbook: Set Up and Run an Organization's Data Supply Chain 1st ed., 2020.	1	
	Rotenberg M., Scott J.,Horwitz, J. Privacy in the Modern Age : The Search for Solutions, 2015.	1	
	Solove D.J., Understanding Privacy, 2009.	1	
	ISO 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines		DA
2.11. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)	1. Leichter, W., Berman., D. Global guide to data protection laws : understanding privacy and compliance requirements in more than 80 countries, 2017. 2. Bazzell, M., Carroll, J. The complete privacy & security : desk reference, 2016. 3. Information Privacy A Complete Guide - 2021 Edition, 2020.		

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Marin Golub Ivan Magdalenić Marcel Maretić	1.6. Godina studija	1
1.2. Naziv predmeta	**Primijenjena kriptografija i sustavi sigurnosti**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici	Marko Hölbl	1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20+0+10+0
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	1
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Upoznati polaznike s kriptografskim metodama, tehnikama i alatima te načinom uporabe ove discipline u sustavima informacijske sigurnosti. Postiže se kroz: • razumijevanje ove discipline i njeno pozicioniranje u cjelovitim sustavima informacijske sigurnosti. • znanje kriptografskih metoda, tehnika i alata, kao i njihovih prednosti i nedostataka kao i praktična primjena ove discipline.		

	• analiziranje i prepoznavanje razloga koji nalažu primjenu ove discipline. • sintetiziranje spoznaja o ovoj disciplini, odabir potrebnih kriptografskih mehanizama te vrednovanje provedenih mjera.
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 4. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 5. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 6. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Valorizirati značaj kriptografije u računalnim sustavima i kako kriptografija utječe na sigurnost informacija. 2. Preporučiti kriptografske metode, tehnike i alate, njihove podjele te prednosti i nedostataka 3. Vrednovati adekvatne kriptografske metode u konkretnom slučaju u praksi 4. Odabrati odgovarajuće kriptografske metode u konkretnom slučaju u praksi Kompetencije: • K1 moguće sigurnosne prijetnje • K2 tehnike izvođenja računalnih napada i mjere za njihovo izbjegavanje • K3 najbolje prakse i norme u upravljanju informacijskom sigurnošću • K4 nadolazeće tehnike i njihove dostupne implementacije
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Ciljevi, taksonomija i funkcije kriptografije i kriptoanalize u informacijskoj sigurnosti. Matematičke osnove. Jednosmjerna funkcija. Permutacija. Involucija. Enkripcijska i deskripcijska funkcija i transformacija. Teorija informacija. Entropija. Enkripcijska shema. Šifra. Definicija probojnosti šifre. Pseudo-slučajni brojevi. (2 sata) Simetrični algoritmi kriptiranja. Definicija simetričnog ključa. Blokovska šifra. Randomizirana šifra. Jednokratna bilježnica (One-Time-Pad, OTP). Simetrični kriptosustavi: DES, 3DES, IDEA, i AES. Substitucijska šifra. Klasične šifre. Mono-alfabetske substitucije. Polialfabetske substitucije. Transpozicijska šifra. Operacije nad šiframa. Kompozicija šifara. Produkt šifara. Protočna šifra. Sinkrona protočna šifra. Binarno aditivna protočna šifra. Asinkrona protočna šifra. Vernamova šifra. Primjena programskih alata zasnovanih na simetričnoj kriptografiji. (2 sata) Digitalni potpis, pečat i žig. Shema digitalnog potpisa DSS i DSA. Procedura potpisivanja i provjere potpisa. RSA shema digitalnih potpisa. Fiat-Shamirova shema digitalnih potpisa. Slijepi potpis. (2 sata) Autentikacija i identifikacija. Zaporke. Fiksne sheme zaporki. Zaporke na operacijskom sustavu UNIX. Pinovi i ključevi. Jednokratne zaporke. Chellange-response identifikacija. Vremenske zamke. Chellange-response pomoću simetričnih ključeva. Chellange-response pomoću javnih ključeva. Primjena kriptografskih alata. (2 sata) Javni i privatni ključevi. Enkripcijska shema javnog ključa. Konstrukcija enkripcijske sheme javnog ključa. Usporedba javnih ključeva i simetričnih ključeva. Provjera primanosti i pseudoprimalnosti broja. Generiranje prostih brojeva. RSA enkripcija.

	Rabinova enkripcija. ElGammal enkripcija. McEliece enkripcija. Enkripcije na temelju problema ranca. Probabilističke enkripcije. Asimetrični kriptografski algoritmi zasnovani na eleptičkim krivuljama: EC ElGamalov kriptosustav i ECDH. Primjena konkretnih alata. (2 sata) Funkcije za izračunavanje sažetka poruke (hash funkcije). Jednosmjerne funkcije i kompresija funkcija. Klasifikacija hash-funkcija. MAC hash funkcije. Porodica funkcija za izračunavanje sažetka poruke SHA s naglaskom na aktualnu funkciju SHA-3. Napadi na hash funkcije. Primjena konkretnih alata. (2 sata) Protokoli i mehanizmi. Kriptografski protokol. Neuspjeh protokola ili mehanizma. Identifikacijski protokoli. Feige-Fiat-Shamirov protokol. GQ protokol. Schnorrov protokol. Napadi na protokole. Protokoli za razmjenu simetričnih ključeva. (2 sata) Uspostava, upravljanje i certifikacija ključeva. Ključevi temeljeni na simetričnoj enkripciji. Ključevi temeljeni na enkripciji javnih ključeva. Tehnike distribucije tajnih ključeva. Tehnike distribucije javnih ključeva. Tehnike kontrole korištenja ključeva. Primjena konkretnih alata i protokola: SSH, SSL i TLS. (2 sata) Kvantna kriptografija. Osnove kriptoanalize. Klase napada na sigurnost. Pasivni napadi. Aktivni napadi. Napadi na enkripcijske sheme. Napadi na protokole vremenski napadi, rođendanski napad, zadržavanje sadržaja memorije i drugo. Modeli vrednovanja kriptografske sigurnosti. (2 sata) Linearna i diferencijalna kriptoanaliza. Napadi koji koriste sporedna fizikalna svojstva kriptografskih funkcija (engl. Side-Channel Attacks, SCA). Jednostavna analiza potrošnje električne energije. (2 sata) Prezentacija i obrana samostalnih projekata (5 sati).

2.6. Vrste izvođenja nastave:	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ *on line* u cijelosti ☐ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☐ mentorski rad ☐ (ostalo upisati)	2.7. Komentari:
2.8. Obveze studenata	Sudjelovanje u diskusijama i obrana projektnog zadatka.		

2.9. Praćenje rada studenata	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		
	Kolokvij			Seminarski rad			(ostalo upisati)		
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**	

2.10. Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	**Naslov**	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**
	Schneier, B.: Applied Cryptography, 2nd ed.: Protoclos, Algorithms, and Source Code in C. John Wiley & Son. 1996	1	

	Menzes, A.; Oorshot, P. van; Vanstone, S.: Handbook of Applied Cryptography, CRC Press, 1996	1	
2.12. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)	• Schneier, B.: Secrets & Lies, John Wiley & Sons, 2000 • Schneier, B.: Practical Cryptography, John Wiley & Sons, 2003		

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1Nositelj predmeta	Melita Kozina Mario Žgela	1.6 Godina studija	1
1.2.Naziv predmeta	**Revizija i kontrola informacijskih sustava**	1.7 Broj bodova po ECTS sustavu	6
1.3Suradnici	Valentina Kirinić	1.8 Način izvođenja nastave (broj sati P + V + S + e-učenje)	20 + 0 + 10
1.4.Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.9 Očekivani broj studenata na predmetu	10 - 15
1.5 Status predmeta	Obavezni	1.10 Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10%
2. OPIS PREDMETA			
2.1 Ciljevi predmeta	Cilj predmeta jest upoznati se s ključnim pojmovima, konceptima, normama, metodama i alatima iz područja Revizije i kontrole informacijskih sustava te ukazati na potrebu primjene ove discipline u praksi i njen značaj za svaki poslovni sustav. Cilj je da studenti nauče prepoznati probleme ovog područja te ovladaju metodama njihovog rješavanja, posebno kako provesti reviziju i kontrolu najznačajnijih komponenti informacijskog sustava. Tri su osnovna smjera razvoja ove discipline. Prvi jest činjenica jest spoznaja da (visoke) investicije u IT neće automatski rezultirati (nikakvim) poslovnim učincima, da se desi pozitivna korelacija, nužni su odgovarajuće znanje i odgovornosti. Drugo, informacijski sustavi postaju i sami predmetom obveznih revizijskih i kontrolnih postupaka. Treći smjer jest primjena informatičkih metoda i programske opreme u reviziji poslovnih sustava, poznavanje i primjena standarda, metoda, tehnika i alata koji se koriste u reviziji i kontroli informacijskih sustava, analiza i prepoznavanje razloga zbog kojih je nužno uspostavljati sustave revizije i kontrole informacijskih sustava kao i načina postupne izgradnje takvih sustava, sinteza i prezentacija programa uvođenja sustava revizije i kontrole informacijskih sustava u poslovanje, vrednovanje uspješnosti uspostavljenog sustava revizije i kontrole informacijskih sustava u praksi.		

2.2 Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Procijeniti utjecaj sigurnosne strategije, sigurnosnih politika, zakonskog okvira, primijenjenih sigurnosnih rješenja na poslovni/ informacijski sustav, te pripadajući sustav informacijske sigurnosti. 2. Analizirati resurse informacijskog sustava s aspekta njihove ranjivosti i sigurnosnih nedostataka. 3. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava. 4. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti. 5. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture. 6. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava, zaposlenici, klijenti, institucije državne uprave).
2.4 Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Poznavati, razumjeti, odabrati i primijeniti standarde, metode, tehnike i alate za reviziju i kontrolu informacijskih sustava. 2. Analizirati i prepoznavati razloge zbog kojih je nužno uspostavljati sustave revizije i kontrole informacijskih sustava kao i načine postupne izgradnje takvih sustava. 3. Sintetizirati i prezentirati programe uvođenja sustava revizije i kontrole informacijskih sustava u poslovanje. 4. Vrednovati uspješnost uspostavljenog sustava revizije i kontrole informacijskih sustava u praksi.
2.5.Sadržaj predmeta	Tema 1 (3 sata): IT Governance kao koncept korištenja IT-a. Razvoj zrelosti korištenja IT-a. Prerastanje „nižih“ koncepata, kao što su ITIM (IT Infrastructure Management) i ITSM (IT Service Management) u IT Governance. IT Governance kao koncept korištenja IT-a. Potreba za ovim konceptom. EDC (Evaluate, Direct, Control) ciklus IT Governance-a. Modeli IT Governance-a: ISO 38500, ITIL, COBIT i drugi modeli korporativnog upravljanja. Učinci primjene koncepta IT Governance-a. Strateško upravljanje IT-em. Ostvarenje poslovnih benefita putem IT-a. Upravljanje poslovnim rizicima zbog IT-a. Optimizacije IT resursa. Tema 2 (4 sata): COBIT (Control of Objectives and Related Technology in IT) kao model revizije IS-a. Namjena i korisnici COBIT-a. Ustrojstvo, ciljevi, principi i način korištenja COBIT-a. Procesi domene EDM (Evaluate, Direct, Monitor). Procesi domene APO (Align, Plan, Organize). Procesi domene BAI (Build, Acquire, Implement). Procesi domene DSS (Delivery, Service, Support). Procesi domene MES (Monitor, Evaluate, Assess). Tema 3 (2 sata): Potreba za revizijom i kontrolom IS-a kao dio IT Governance-a. Razlozi koji su doveli do nužnosti za revizijom i kontrolom IS-a. Analize slučajeva iz prakse. Međunarodni standardi i metode za postupke revizije i kontrole IS-a (ISACA, COBIT, COSO, SOX,ISO 27001, ISO 20000, ISO 22301 i dr.). Nacionalni propisi i norme za reviziju i kontrolu IS-a. Korisnici rezultata revizija i kontrola. Međunarodne asocijacije u ovom području (ISACA i dr.). Najbolja praksa za reviziju i kontrolu IS.

	Tema 4 (3 sata): Proces revizije IS-a, potrebna znanja i odgovornosti. ISACA pristup reviziji i kontroli IS-a. ISACA standardi reviziji IS-a. Područja i vrste revizija i kontrola IS-a. Proces revizije IS-a. Potrebna znanja i odgovornost revizora. Zahtjevi za revizijom odgovornosti za IT – odgovornost korporativne razine, odgovornost razine izvršnog poslovodstva, odgovornost za IT na operativnoj razini. Tema 5 (5 sata): Detaljni prikaz načina revizije nekih vitalnih područja IS-a: životnog ciklusa, poslovnih aplikacija, tehničke infrastrukture i baza podataka. Revizija planiranja poslovnih aplikacija, razvoja, nabave, implementacije i održavanja IS-a. Revizija aplikacijskih kontrola, revizija odnosa funkcija projektiranja, programiranja i održavanja aplikacija. Revizija strojne i mrežne opreme: poslužitelja, osobnih računala, sistemske i komunikacijske programske opreme, sustava za otkrivanje upada, vatrozidnih sustava. Revizija odnosa s dobavljačima. Revizija baza podataka: integriteta, pristupnih prava, nadzora korisničkog rada, visoke raspoloživosti, izrade rezervnih kopija, odnosa s operativnim sustavom, nadzora rada i oporavka baza podataka, izvještavanja itd. Prikazi različitih primjera. Pravni aspekti revizije IS-a- primjeri revizije ugovora između dobavljača i korisnika IT usluga. Tema 6 (6 sati): Revizija sustava informacijske sigurnosti, sustava za upravljanje kontinuitetom poslovanja i rada kritičnih komponenti IS-a. Revizija politika i organizacije informacijske sigurnosti. Revizija upravljanja informacijskom imovinom. Revizija sigurnosti ljudskih resursa, fizičke sigurnosti i sigurnosti okruženja. Revizija komunikacija, operative i kontrola pristupa. Revizija upravljanja sigurnosnim incidentima i revizija sukladnosti. Revizija analize i procjene poslovnih rizika, te planova za prevenciju i oporavak. Revizija implementacije, testiranja i održavanja sustava za upravljanje kontinuitetom poslovanja. Revizija organizacijske strukture za upravljanje kontinuitetom poslovanja. Programska oprema za potporu upravljanju kontinuitetom poslovanja. Tema 7 (5 sati): Analize podataka korištenjem računalno podržanih revizijskih alata (primjeri IDEA CAAT). Svrha uporabe takovih alata, područja primjene, uporaba statističkih i matematičkih funkcija, specijalizirane tehnike analize podataka (raslojavanje, otkrivanje praznina itd.), selekcija sumnjivih transakcija. Samostalan rad polaznika u računalskoj analizi nekih baza podataka korištenjem SQL upitnog jezika i QBE alata. Primjena Benford-ovog zakona u revizijskim postupcima. Tema 8 (2 sata): Upravljanje razvojem zrelosti / sposobnosti iskorištenja IT potencijala u nekom poslovnom sustavu na osnovi postupaka revizija i kontrola IS-a. Načini osvješćivanja uprave, izvršnog menadžmenta, IT osoblja i korisnika o njihovim ulogama u iskorištenju IT potencijala u poslovnom sustavu. IT kao inovacijski potencijal.		
2.6. Vrste izvođenja nastave:	☒ predavanja ☒ seminari ☐ vježbe ☐ on line u cijelosti ☐ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)	2.1. Komentari:
2.7. Obveze studenata	Vježba: izraditi plan revizije informacijskog sustava na primjeru organizacije, s primjerom kriterija revizije i očekivanih sudionika prema područjima revizije		

2.8. Praćenje rada studenata	Pohađanje nastave	**DA**		Projekt			Pismeni ispit		NE
	Eksperimentalni rad		NE	Istraživanje		NE	Usmeni ispit	**DA**	
	Esej		NE	Referat		NE	(ostalo upisati)		NE
	Kolokvij		NE	Seminarski rad	**DA**		(ostalo upisati)		NE
			NE	Praktični zadaci	**DA**		Broj bodova po ECTS sustavu (ukupno)	**6**	

	Naslov	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
2.9. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	Krakar Z. i suradnici „Korporativna informacijska sigurnost, Fakultet organizacije i informatike Sveučilišta u Zagrebu i Zavod za informatiku Hrvatske, Varaždin, 2014.	5	
	M.Kozina**:** Neki aspekti IT menadžmenta u uvjetima digitalne ekonomije, Fakultetski udžbenik, FOI, Varaždin, 2017.	3	
	ISACA ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition		Online
	COBIT 5**:** A Business Framework for the Governance and Management of Enterprise IT, ISACA, 2012.		Online
2.10.Dopunska literatura (navesti naslov)	1. CGEIT Certified in the Governance of Enterprise IT, Firebrand Custom Designd Courseware, 2015. Dostupno na http://www.firebrandtraining.co.uk/pdf/learn/isaca/isaca-crisc-courseware.pdf 2. ISO/IEC 38500 Information technology – Governance of IT for the organization, ISO, 2015. Dostupno na www.iso.org		

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Markus Schatten	1.2. Godina studija	1
1.3. Naziv predmeta	**Sigurnosna pohrana, arhiviranje i repozitoriji podataka**	1.4. Broj bodova po ECTS sustavu	5
1.5. Suradnici	Bogdan Okreša Đurić	1.6. Način izvođenja nastave (broj sati P + V + S + e-učenje)	15+5+10+0
1.7. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.8. Očekivani broj studenata na predmetu	5
1.9. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta on line (maksimalno 20%)	3, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Cilj predmeta je studente upoznati sa specifičnim aspektima upravljanja elektroničkim zapisima, sigurnosne pohrane podataka, elektroničke istrage te analitike velikih količina podataka u kontekstu elektroničkih zapisa i administracije sustava, te kako ti aspekti utječu na cjeloviti sustav sigurnosti informacijskog sustava.		

2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Preporučene ulazne kompetencije za upisivanje predmeta uključuju naprednije poznavanje administracije sustava, skriptnog programiranja, baza i repozitorija podataka, te poznavanje osnova statistike. U idealnom slučaju, student ima prethodno iskustvo administracije sustava u kojem se pojavljuju velike količine podataka.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Uspostaviti i primijeniti planove i procedure za osiguranje informacijske imovine, uključujući i planove oporavka, u skladu s međunarodnim normama, zakonskim aktima i iskustvima dobre prakse. 3. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti 4. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 5. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 6. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 7. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
2.1. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Vrednovati sustav za upravljanje elektroničkim zapisima u konkretnoj organizaciji 2. Kombinirati različite strategije upravljanja elektroničkim zapisima i sigurnosnom pohranom podataka 3. Upravljati incidentima u sustavu za upravljanje elektroničkim zapisima te ostvariti povrat podataka 4. Organizirati proces elektroničke istrage korištenjem odgovarajućih metoda i tehnika upravljanja, identifikacije, očuvanja, prikupljanja, obrade, procjene, analize, produkcije i prezentacije podataka 5. Predložiti odgovarajuće analize velikih količina podataka za povećanje sigurnosti i prevenciju incidentnih situacija
2.2. Sadržaj predmeta	Sadržaj predavanja: • ARHIVIRANJE I UPRAVLJANJE ELEKTRONIČKIM ZAPISIMA - Uvod. Osnove arhiviranja i upravljanja elektroničkim zapisima. Zakonodavni okvir. Standardi i norme. Inventoriji. Taksonomije. Retencija. Metapodaci. Sustavi za upravljanje elektroničkim zapisima. Računalstvo u oblaku i elektronički zapisi. Elektronički zapisi na Internetu i polustrukturirani podaci. Društveni mediji. Strukturirani podaci. Velike količine podataka (BigData). Elektronički zapisi koji predstavljaju komunikaciju (e-mail, drugi komunikacijski mediji). • SIGURNA POHRANA PODATAKA - Uvod. Motivacija za sigurnu pohranu podataka. Strategije sigurne pohrane. Cjelovita pohrana. Inkrementalna pohrana. Mediji za sigurnu pohranu. Alati i tehnologije sigurne pohrane. Upravljanje incidentima i povrat podataka. • E-DISCOVERY - Uvod. Referentni model elektroničke istrage. Upravljanje podacima. Identifikacija. Očuvanje. Prikupljanje. Obrada. Procjena. Analiza. Produkcija. Prezentacija. • ANALITIKA VELIKIH KOLIČINA PODATAKA - Uvod. Izvori podataka. Prikupljanje i indeksiranje podataka. Analiza statičnih podataka. Analiza dinamičkih podataka u stvarnom vremenu. Nadzor podataka u stvarnom vremenu. Vizualizacija podataka i kreiranje izvještaja.

	Sadržaj laboratorijskih vježbi: Tijekom laboratorijskih vježbi analizirat će se studije slučajeva na konkretnim primjerima, a mogu uključivati uspostavu sustava sigurne pohrane odabranom strategijom u odgovarajućoj tehnologiji, simulaciju incidentne situacije s ponovnom uspostavom sustava i povratom podataka, obradu konkretnog slučaja elektroničke istrage (e-discovery) ili analitiku odabranih velikih izvora podataka vezanih uz elektroničke zapise i sustavsku administraciju konkretnog sustava.

2.3. Vrste izvođenja nastave:			2.4. Komentari:
	☒ predavanja ☐ seminari i radionice ☒ vježbe ☐ on line u cijelosti ☐ mješovito e-učenje ☐ terenska nastava	☐ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☐ mentorski rad ☐ (ostalo upisati)	

2.5. Obveze studenata	Studenti su obavezni izraditi praktičan projekt vezan uspostavu sustava sigurnosne pohrane podataka na konkretnom slučaju, ponovno uspostavljanje rada sustava i povrat podataka nakon (simulacije) incidentne situacije, obradu slučaja elektroničke istrage ili analitiku konkretnih velikih izvora podataka vezanih uz elektroničke zapise i sustavsku administraciju. Projektni zadatak se sastoji od praktičnog dijela i dokumentacije te prezentacije projekta. Za polaganje ispita, studenti su obavezni položiti usmeni ispit nakon uspješno obranjenog projekta.

2.6. Praćenje rada studenata									
Pohađanje nastave			Projekt	DA		Pismeni ispit			
Eksperimentalni rad			Istraživanje			Usmeni ispit	DA		
Esej			Referat			(ostalo upisati)			
Kolokvij			Seminarski rad			(ostalo upisati)			
			Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**		

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Smallwood, Robert F. *Managing electronic records: methods, best practices, and technologies*. Vol. 592. John Wiley & Sons, 2013.	1	
	Jacobs, Jay, and Bob Rudis. *Data-Driven Security: Analysis, Visualization and Dashboards*. John Wiley & Sons, 2014.	1	

2.11. Dopunska literatura (navesti naslov)	• Talabis, Mark, et al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014.

	• Mohanty, Hrushikesha, Prachet Bhuyan, and Deepak Chenthati, eds. Big Data: A Primer. Vol. 11. Springer, 2015. • Craig, Terence, and Mary E. Ludloff. Privacy and big data. " O'Reilly Media, Inc.", 2011. • Santos, Omar. *Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security*. Cisco Press, 2015. Mosco, Vincent. *To the cloud: Big data in a turbulent world*. Routledge, 2015. • Elmer, Greg, Ganaele Langlois, and Joanna Redden, eds. *Compromised Data: From Social Media to Big Data*. Bloomsbury Publishing USA, 2015.

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Markus Schatten	1.6. Godina studija	1
1.2. Naziv predmeta	**Sigurnost baza podataka**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici	Bogdan Okreša Đurić	1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20+10+0
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	5
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	3, 10 %
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Cilj predmeta je studente upoznati sa specifičnim aspektima sigurnosti u kontekstu baza podataka. Posebno cilj je polaznicima dati uvid u suvremene metode sigurnosti, zaštite, nadzora, revizije i forenzike baze podataka te prenesti stručna znanja za upravljanje sustavom sigurnosti baze podataka. Uz navedeno, cilj je i ukazati na suvremene trendove u području upravljanja podacima koji se tiču velikih količina podataka (BigData), polustrukturiranih, distribuiranih i NoSQL baza podataka te računalstva u oblaku.		
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Preporučene ulazne kompetencije za upisivanje predmeta uključuju napredno poznavanje relacijskih baza podataka te odgovarajućih sustava za upravljanje bazama podataka, kao i osnovno poznavanje nerelacijskih sustava za upravljanje bazama podataka. U idealnom slučaju, student treba imati praktično iskustvo administracije sustava za upravljanje bazom podataka.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu 2. Uspostaviti i primijeniti planove i procedure za osiguranje informacijske imovine, uključujući i planove oporavka, u skladu s međunarodnim normama, zakonskim aktima i iskustvima dobre prakse. 3. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti 4. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 5. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 6. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti.		

	7. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.		
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Kritički prosuđivati moguće prijetnje sigurnosti baze podataka 2. Izraditi prijedlog višerazinskog sustava sigurnosti baze podataka u kontekstu sustava informacijske sigurnosti organizacije 3. Upravljati incidentnim situacijama u sustavu za upravljanje bazom podataka. 4. Predložiti rješenje oporavka baze podataka 5. Sastaviti forenzičku analizu konkretne baze podataka 6. Predložiti sustav nadzora baze podataka i upravljati revizijom baze podataka 7. Argumentirati mišljenje o izazovima suvremenih sustava za upravljanje bazama podataka uključujući NoSQL, BigData i distribuirane baze podataka		
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Sadržaj predavanja 1. UVOD – Baze podataka i sigurnost. Motivacija za uvođenje sigurnosti baze podataka. Osnovni koncepti sigurnosti u bazama podataka. Prijetnje bazama podataka. Razine sigurnosti baze podataka. (1 sat) 2. ARHITEKTURA SIGURNOSTI BAZE PODATAKA – Sigurnost na razini operacijskog sustava. Sigurnost na razini računalne mreže. Sigurnost na razini sustava za upravljanje bazom podataka. Kontrola pristupa. Upravljanje korisničkim računima, lozinkama, privilegijima i ulogama. Enkripcija, skrivanje i sigurnosno označavanje podataka. Virtualno privatne baze podataka. Aplikacijska sigurnost. Testiranje sigurnosti baze podataka. Detekcija napada. (5 sati) 3. FORENZIKA BAZA PODATAKA – Upravljanje incidentnim situacijama. Metapodaci i sistemski katalog. Post-mortem analiza. Live analiza. Hibridne analize. Rudarenje podataka. Pronalaženje uzoraka u bazama podataka. Statističke i temporalne analize. Oporavak baze podataka. (4 sata) 4. NADZOR I REVIZIJA BAZA PODATAKA – Uspostava sustava revizije baze podataka. Modeli revizije baza podataka. Politika sigurnosti baza podataka. Revizija provjere pristupa bazi podataka. Revizija korisnika i administratora baze podataka. Sigurnosni nadzor aktivnosti. Revizija ranjivosti i prijetnji bazi podataka. Upravljanje promjenama u bazi podataka. Najbolje prakse revizije baza podataka. (2 sata) 5. NAPREDNE TEME – Sigurnost distribuiranih baza podataka. NoSQL i sigurnost. Polustrukturirani podaci (XML, JSON, RDF) i sigurnost. BigData i sigurnost. Tokovi podataka (engl. stream based data) i sigurnost. Sigurnost objektno-orijentiranih baza podataka. (3 sata) Sadržaj laboratorijskih vježbi Studija slučaja odabranog sustava za upravljanje bazom podataka koji može uključivati instalaciju i konfiguraciju sustava sigurnosti, uspostavu sigurnosnih mehanizama, implementaciju virtualne privatne baze podataka, testiranje sigurnosti baze podataka i aplikacijske sigurnosti, forenzičku analizu konkretnog slučaja. (5 sati)		
2.6. Vrste izvođenja nastave:	☒ predavanja	☒ samostalni zadaci	2.7. Komentari:

	☐ seminari i radionice ☒ vježbe ☐ *on line* u cijelosti ☐ mješovito e-učenje ☐ terenska nastava	☐ multimedija i mreža ☐ laboratorij ☐ mentorski rad ☐ (ostalo upisati)
2.8. Obveze studenata	Studenti su obavezni izraditi praktičan projekt vezan uz sigurnost konkretnog sustava za upravljanje bazom podataka koji se može ticati uspostave sustava sigurnosti, testiranja sigurnosti i/ili forenzičke analize. Projektni zadatak se sastoji od praktičnog dijela i dokumentacije te prezentacije projekta. Za polaganje ispita, studenti su obavezni položiti usmeni ispit nakon uspješno obranjenog projekta.	

2.9. Praćenje rada studenata									
	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		
	Kolokvij			Seminarski rad			(ostalo upisati)		
				Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)		

2.10. Obvezna literatura (dostupna u knjižnici i7ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Basta, A., & Žgela, M. (2011). *Database security*. Cengage Learning.	1	

2.11. Dopunska literatura (navesti naslov)	
	• Gertz, Michael, and Sushil Jajodia, eds. *Handbook of database security: applications and trends*. Springer Science & Business Media, 2007. • Litchfield, David. *The Database Hacker's Handbook: Defending Database Servers*. John Wiley & Sons, 2005.

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Boris Tomaš Neven Vrček	1.6. Godina studija	1

1.2. Naziv predmeta	**Sigurnost interneta stvari (IoT)**	1.7. Broj bodova po ECTS sustavu	5
1.3. Suradnici	Luka Milić.	1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	20+0+10
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Kroz predmet Sigurnost interneta stvari studenti će se upoznati sa sigurnosnim, regulatornim i tehničkim izazovima implementacije i korištenja Interneta stvari (dalje u tekstu: IoT, eng. Internet of Things) gdje pametni uređaji u današnjem svijetu djeluju kao prijelaz između digitalnog i fizičkog okruženja. IoT se dotiče mnogih aspekata današnjeg života, uključujući prijevoz, zdravstvenu zaštitu, sigurnost, okoliš, energiju, te njihovu primjenu nalazimo u različitim industrijskim vertikalama. Nalazimo ga u obliku rješenja za tzv. pametne kuće, pametni gradovi, inteligentni javni prijevoz, pametni sustavi napajanja, pametni automobili, pametni aerodromi, e-zdravstvo, pametne bolnice i sl. Studenti će razmotriti principe sigurnosti u dizajnu IoT rješenja i usluga, od rane faze njihovog arhitekturalnog dizajna do konačne implementacije. Kroz studije slučajeva razmatrati će se ranjivosti i prijetnje u domeni IoT sigurnosti, te moguće posljedice IoT sigurnosnih incidenata, uključujući ekonomska i etička pitanja, te povrede privatnosti i zaštite osobnih podataka.		
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata razvoja informacijskog sustava i implementacije mjera informacijske sigurnosti; osnove procjene i upravljanja rizicima informacijske sigurnosti.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom dizajna i implementacije kontrola informacijske sigurnosti u razvoju i implementaciji interneta stvari 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i implementacije IoT rješenja i usluga 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti i zaštite privatnosti 4. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka i programska rješenja za sigurno IoT okruženje 5. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite IoT okruženja s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih sigurnosnih kontrola		
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Analizirati sigurnosna, ekonomska, društvena i etička pitanja vezana uz Internet stvari 2. Primijeniti metode identifikacije i analize sigurnosnih rizika vezanih uz Internet stvari 3. Predložiti sigurnosne kontrole za mitigaciju sigurnosnih rizika vezanih uz Internet stvari 4. Vrednovati izvedene aktivnosti tijekom realizacije kolegija		
2.5. Sadržaj predmeta	Uvod u Internet stvari. Uvod u sigurnost Interneta stvari. Mogućnosti primjene Interneta stvari (pametne kuće, pametni gradovi, inteligentni javni prijevoz, pametni sustavi napajanja, pametni automobili, pametni aerodromi, e-zdravstvo, pametne bolnice i sl.).		

<table>
<tr><td></td><td colspan="9">Razmatranja sigurnosti Interneta stvari kroz sve faze njegovog dizajna, razvoja i implementacije, s aspekta razvoja uređaja i aplikacija.
Integracija smjernica, koncepata i najboljih praksi sigurnosti i privatnosti (security by design, privacy by design) u razvoj Interneta stvari.
Sigurnosne politike, etička i regulatorna pitanja vezana uz Internet stvari.
Rizici korištenja Interneta stvari vezani uz sigurnost ljudskih života i sigurnost fizičkog okruženja.
IT sigurnosna arhitektura Interneta stvari. Dizajn arhitekture sustava u cilju sprečavanja sigurnosnih napada i iskorištavanja potencijalih ranjivosti.
Prepoznavanje i utvrđivanje informacijske imovine uključene u Internet stvari (pristupni, endpoint uređaji, kućna mreža, roaming mreže, servisne platforme itd.).
Metode provjere sigurnosti, penetracijska testiranja, identifikacije ranjivosti interneta stvari.
Identifikacija i procjena rizika interneta stvari. Identifikacija i primjena organizacijskih i tehničkih sigurnosnih kontrola za upravljanje rizicima IoT-a prema svim primjenjivim domenama međunarodnih standarda za upravljanje informacijskom sigurnošću (ISO, NIST, OWASP itd).
Autentićnost zapisa u arhitekturi interneta stvari. Povezanost s blockchain tehnologijama.
Procjena učinka na zaštitu osobnih podataka pri korištenju Interneta stvari u različitim industrijskim vertikalama.
Identifikacija rizika u lancu opskrbe za razvoj IoT rješenja i usluga. Način reguliranja odnosa s dobavljačima obzirom na sigurnosne zahtjeve. Sigurnosne certifikacije dobavljača (EU/ENISA okvir, ISO 27001, itd.)
Studije slučajeva na temelju poznatih sigurnosnih incidenata. Razmatranje posljedica IoT incidenata, uključujući ekonomska i etička pitanja, te povrede privatnosti i zaštite osobnih podataka.</td></tr>
<tr><td>2.6. Vrste izvođenja nastave:</td><td colspan="3">☒ predavanja
☒ seminari i radionice
☐ vježbe
☐ on line u cijelosti
☒ mješovito e-učenje
☐ terenska nastava</td><td colspan="3">☒ samostalni zadaci
☐ multimedija i mreža
☐ laboratorij
☒ mentorski rad
☐ (ostalo upisati)</td><td colspan="3">2.7. Komentari:</td></tr>
<tr><td>2.8. Obveze studenata</td><td colspan="9">Vježba: Analizirati i usporedite okruženje Interneta stvari po pitanju sigurnosnih prijetnji i ranjivosti obzirom na specifičnosti pojedine industrije i tehnoloških karakteristika razmatrane vrste uređaja</td></tr>
<tr><td rowspan="4">2.9. Praćenje rada studenata</td><td>Pohađanje nastave</td><td>DA</td><td></td><td>Projekt</td><td>DA</td><td></td><td>Pismeni ispit</td><td>DA</td><td></td></tr>
<tr><td>Eksperimentalni rad</td><td></td><td></td><td>Istraživanje</td><td></td><td></td><td>Usmeni ispit</td><td>DA</td><td></td></tr>
<tr><td>Esej</td><td></td><td></td><td>Referat</td><td></td><td></td><td>(ostalo upisati)</td><td></td><td></td></tr>
<tr><td>Kolokvij</td><td></td><td></td><td>Seminarski rad</td><td></td><td></td><td>(ostalo upisati)</td><td></td><td></td></tr>
</table>

				Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)	**5**

	Naslov	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
2.1. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017		DA
	ENISA, Good practices for security of IoT, Secure Software Development Lifecycle, November 2019		DA
	Russell, Brian, and Drew Van Duren. Practical internet of things security. Packt Publishing Ltd, 2016.	1	
2.11. Dopunska literatura (navesti naslov)	• Dhanjani, Nitesh. Abusing the internet of things: blackouts, freakouts, and stakeouts. " O'Reilly Media, Inc.", 2015. • Gupta, Aditya. The IoT Hacker's Handbook. Apress, 2019. • Smith, Sean. The Internet of Risky Things: Trusting the devices that surround us. " O'Reilly Media, Inc.", 2017.		

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Ivan Magdalenić Marin Golub	1.6. Godina studija	
1.2. Naziv predmeta	**Sigurnost operacijskih sustava**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici		1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	15+0+15+0
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	2, 20%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Upoznati polaznike s potrebom sigurnosti operacijskih sustava i naučiti ih primjeni metoda i kontrolnih mehanizama putem kojih se ona postiže. Realizira se kroz: • Razumijevanje potrebe zaštite operacijskih sustava i posljedica neadekvatne zaštite. Poznavanje sigurnosnih sredstava i mehanizama, načina implementacije i ostvarenja zaštite u takvim sustavima. • Poznavanje metodike i prakse sigurnosti operacijskih sustava i pouzdanosti i raspoloživosti sustava. Sigurnosne funkcije, razine i način implementacije.		

	• Prepoznavanje opasnosti od zlonamjernih upada i napada u operacijske sustave, posebice putem interneta (npr. DoS, DDoS), zlonamjernih kodova (virusi, zombiji, crvi,...) i načini obrane od njih (provjera vjerodostojnosti, kontrola pristupa, vatroštit,...). • Primjena suvremenih kontrolnih mjera za usluge operacijskih sustava, putem kojih se postiže pouzdanost, integritet, tajnost i prava pristupa. Primjena sigurnosnih alata i mehanizama u operacijskim sustavima.
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Preporuka je biti upoznati s osnovama rada operacijskih sustava i kriptografskim tehnikama.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Uspostaviti i primijeniti planove i procedure za osiguranje informacijske imovine, uključujući i planove oporavka, u skladu s međunarodnim normama, zakonskim aktima i iskustvima dobre prakse. 3. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti. 4. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 5. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 6. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	7. Kritički prosuđivati značaj i odgovornosti uvođenja mjera sigurnosti i zaštite kod operacijskih sustava. 8. Valorizirati standard, mehanizme i sustave sigurnosti. 9. Analizirati uvođenje pojedinačnih sigurnosnih funkcija, predlaganje eventualnih poboljšanja i uspostava sustava sigurnosti. 10. Preporučiti korake, prioritete, učinke i načine uspostave sigurnosti operacijskih sustava. 11. Vrednovanje djelotvornosti predloženih mjera i načina njihove implementacije. 12. Argumentirati odabir sigurnosnih mehanizma i normi za ostvarivanje i unapređivanje sigurnosti operacijskih sustava. Kompetencije: • K1 funkcionalna specifikacija informacijskih sustava • K2 primjena postojećih tehničkih arhitektura u informacijskim i komunikacijskim tehnologijama • K3 kako su poslovni procesi integrirani u programskoj podršci IKT-a i njihova međuzavisnosti • K4 promjena alata i tehnika koji se koriste za upravljanje • K5 najbolje prakse i norme u upravljanju informacijskom sigurnošću • K6 relevantni izvori informacija (npr. časopisi, konferencije, događaji, forumi i ostale publikacije) • K7 tehnike izvođenja računalnih napada i mjere za njihovo izbjegavanje • K8 moguće sigurnosne prijetnje • K9 tehnike otkrivanja sigurnosnih napada • K10 uređaji i alati za pohranu i dohvaćanje podataka Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: • (ISC)2 SSCP – Systems Security Certified Practitioner
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Procjena rizika na razini operacijskog sustava • Pregled postojećeg stanja i načini poboljšavanja sigurnosti, identifikacija ranjivosti operacijskog sustava, identifikacija nepotrebnih IT servisa i datoteka uključenih u operacijski sustav, identifikacija otvorenih komunikacijskih portova,

<table>
<tr><td></td><td colspan="8">identifikacija korisničkih računa s pravima pristupa operacijskom sustavu, identifikacija učinkovitosti postojećih metoda zaštite (vatroštit, antivirus).

Ostvarivanje sigurnosnih mehanizama u operacijskim sustavima
• Pregled kriptografskih tehnika.
• Primjena enkripcije u zaštiti korisničkih računa, zaporke, višefaktorna autentikacija, korisnički certifikati, primjena smart kartica.
• Lozinke, ACL, prava pristupa
• Sigurnosne politike na razini operacijskih sustava
• Izrada sigurnosnih kopija, replikacija
• Višediskovni zalihosni sustavi, osnove sustava visoke raspoloživosti, georedundancija, izgradnja IT sustava u oblaku, hibridni IT sustavi (on-premisse/cloud)
• Vatroštit

Napadi na operacijski sustav
• Klasifikacija napada
• Metode prikrivanja napada
• Metode otkrivanja i sprečavanja napada
• Alati za održavanje sigurnosti
• Uspostavljanje sustavne spremnosti za odgovor na kibernetički napad, definiranje odgovornosti i procedura za odgovor na incidente
• Učenje na incidentima

Studija slučaja (10 sati)
• Implementacija sigurnosti na razini operacijskog sustava u stvarnom poduzeću. Obrada dva studija slučaja.

Prezentacija i obrana samostalnih projekata (5 sati).</td></tr>
<tr><td>2.6. Vrste izvođenja nastave:</td><td colspan="3">☐ predavanja
☒ seminari i radionice
☐ vježbe
☐ on line u cijelosti
☐ mješovito e-učenje
☐ terenska nastava</td><td colspan="3">☐ samostalni zadaci
☐ multimedija i mreža
☐ laboratorij
☒ mentorski rad
☐ (ostalo upisati)</td><td colspan="2">2.7. Komentari:</td></tr>
<tr><td>2.8. Obveze studenata</td><td colspan="8">Vježbe: Studije slučaja</td></tr>
<tr><td>2.9. Praćenje rada studenata</td><td>Pohađanje nastave</td><td>DA</td><td></td><td>Projekt</td><td>DA</td><td></td><td>Pismeni ispit</td><td></td><td>NE</td></tr>
</table>

	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		NE
	Kolokvij			Seminarski rad	DA		(ostalo upisati)		NE
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**	

	Naslov	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**
2.11. Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	L. Budin, M. Golub, D. Jakobović, L. Jelenković, Operacijski sustavi, izdavač Element, Zagreb, 2010.	3	
	Tannenbaum, A. S. Modern Operating Systems, forth edition, Prentice Hall, 2014.	1	
2.12. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)			

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Ivan Magdalenić Nikola Ivković Muhamed Turkanović	1.6. Godina studija	1
1.2. Naziv predmeta	Sigurnost umreženih računalnih sustava	1.7. Broj bodova po ECTS sustavu	5
1.3. Suradnici	Luka Milić	1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	15+0+15+0
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	1
2. OPIS PREDMETA			

2.1. Ciljevi predmeta	Upoznati polaznike s potrebom sigurnosti umreženih računalskih sustava i naučiti ih primjeni metoda i kontrolnih mehanizama putem kojih se ona postiže. Realizira se kroz: • Razumijevanje potrebe sigurne komunikacije u uvjetima umreženih računalskih sustava. Poznavanje sigurnosnih sredstava i mehanizama, načina implementacije i ostvarenja zaštite u takovim sustavima. • Poznavanje metodike i prakse sigurnosti računalnih sustava, distribuiranih sustava i interneta. Sigurnosne funkcije, razine i način implementacije. • Prepoznavanje opasnosti od zlonamjernih upada i napada u umrežene računalske sustave, posebice putem interneta (npr. DoS, DDoS), zlonamjernih kodova (virusi, zombiji, crvi,...) i načini obrane od njih (provjera vjerodostojnosti, kontrola pristupa, virtualne privatne mreže, vatrozidovi,...). • Primjena suvremenih kontrolnih mjera za mrežne usluge, putem kojih se postiže tajnost, cjelovitost, vjerodostojnost i neodbijanje. Primjena sigurnosnih alata i mehanizama u internet protokolima i aplikacijama, kao što su Kerberos, TSL, IPsec, i drugi. Analiza i korištenje često korištenih ostvarenja kriptografije na internetu. Zaštita važnijih aplikacija interneta (web, e-pošta).
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti. Preporuka je biti upoznati s osnovama računalnih mreža i kriptografskim tehnikama.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti. 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 4. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 5. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 6. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Preispitati značaj i odgovornost uvođenja mjera sigurnosti i zaštite kod umreženih računalnih sustava. 2. Preporučiti standarde, mehanizme i sustave sigurnosti. 3. Prezentirati sintetizirane spoznaje o potrebi, koracima, prioritetima, učincima i načinima uspostave sigurnosnog sustava umreženih računalnih sustava. 4. Vrednovati djelotvornost predloženih mjera i načina njihove implementacije. 5. Preispitati sigurnosne mehanizme, protokole i norme za ostvarivanje i unaprjeđivanje sigurnosti umreženih računalnih sustava Kompetencije: • K1 funkcionalna specifikacija informacijskih sustava • K2 primjena postojećih tehničkih arhitektura u informacijskim i komunikacijskim tehnologijama • K3 kako su poslovni procesi integrirani u programskoj podršci IKT-a i njihova međuzavisnosti • K4 promjena alata i tehnika koji se koriste za upravljanje • K5 najbolje prakse i norme u upravljanju informacijskom sigurnošću • K6 relevantni izvori informacija (npr. časopisi, konferencije, događaji, forumi i ostale publikacije) • K7 tehnike izvođenja računalnih napada i mjere za njihovo izbjegavanje

<table>
<tr><td></td><td colspan="9">• K8 moguće sigurnosne prijetnje
• K9 tehnike otkrivanja sigurnosnih napada

Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima:
• (ISC)2 SSCP – Systems Security Certified Practitioner</td></tr>
<tr><td>a. Sadržaj predmeta</td><td colspan="9">Procjena rizika umreženim računalnim sustavima
• Razumijevanje ranjivosti umreženih računalnih sustava.
• Tipični vektori napada na umrežene računalne sustave.
• Strategije napada.
• Upoznavanje s postojećim katalozima sigurnosnih rizika.
• Pregled postojećeg stanja i načini poboljšavanja sigurnosti.
• Identifikacija ranjivosti u dizajnu i arhitekturi sustava.
• Identifikacija ranjivosti u elementima sustava.
• Procjena rizika i definiranje plana za njihovo umanjivanje.

Ostvarivanje sigurnosnih mehanizama u umreženim sustavima
• Dizajn sigurnosti umreženih sustava
• Pregled kriptografskih tehnika.
• Sigurnosni protokoli (TLS, IPsec, DNS security, DTLS…)
• Postupci ostvarivanja mrežne sigurnosti.
• Vatroštit, VPN, IDS, IPS, DMZ
Studija slučaja
• Implementacija mrežne sigurnosti u stvarnom poduzeću. Obrada dva studija slučaja.
Prezentacija i obrana samostalnih projekata</td></tr>
<tr><td>b. Vrste izvođenja nastave:</td><td colspan="3">☒ predavanja
☒ seminari i radionice

☐ vježbe
☐ on line u cijelosti
☐ mješovito e-učenje
☐ terenska nastava</td><td colspan="3">☒ samostalni zadaci
☐ multimedija i mreža
☐ laboratorij
☒ mentorski rad

☐ (ostalo upisati)</td><td colspan="3">c. Komentari:</td></tr>
<tr><td>d. Obveze studenata</td><td colspan="9">Vježbe: Implementacija mrežne sigurnosti u stvarnom poduzeću. Obrada dva studija slučaja.</td></tr>
<tr><td rowspan="4">e. Praćenje rada studenata</td><td>Pohađanje nastave</td><td>DA</td><td></td><td>Projekt</td><td>DA</td><td></td><td>Pismeni ispit</td><td></td><td>NE</td></tr>
<tr><td>Eksperimentalni rad</td><td></td><td></td><td>Istraživanje</td><td>DA</td><td></td><td>Usmeni ispit</td><td>DA</td><td></td></tr>
<tr><td>Esej</td><td></td><td></td><td>Referat</td><td></td><td></td><td>(ostalo upisati)</td><td></td><td>NE</td></tr>
<tr><td>Kolokvij</td><td></td><td></td><td>Seminarski rad</td><td>DA</td><td></td><td>(ostalo upisati)</td><td></td><td>NE</td></tr>
</table>

				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	

	Naslov	Dostupnost u knjižnici	Dostupnost putem ostalih medija
2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	Andrew S. Tanenbaum, David J. Wetherall, Computer Networks 6/E, Pearson, 2021.	1	
	Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, ONLINE: https://book.systemsapproach.org, 2020.	N/A	
	James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach 8/E, Pearson, 2020.	1	
2.11. Dopunska literatura (navesti naslov)	• William Stallings, Cryptography and Network Security: Principles and Practice, 6/E, Pearson, 2014. • Forshaw, James. Attacking network protocols: a hacker's guide to capture, analysis, and exploitation. No Starch Press, 2017. • Gilman, Evan. Zero Trust Networks: Building Systems in Untrusted Networks, 2016.		

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Dragutin Kermek Muhamed Turkanović Marko Hölbl	1.6. Godina studija	1
1.2. Naziv predmeta	Sigurnost web i poslužiteljskih aplikacija	1.7. Broj bodova po ECTS sustavu	5
1.3. Suradnici	Matija Novak	1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	20 + 0 + 10
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Naučiti polaznike metode i načine podizanja razine sigurnosti suvremenih poslužiteljskih i web aplikacija. Prikazati česte klase ranjivosti i načine neutralizacije ranjivosti koje su vezane uz aplikacijsku sigurnost i mogućnost neovlaštene modifikacije toka izvršavanja aplikacije.		
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.		

2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti. 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti 4. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 5. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Kritički prosuđivati klase ranjivosti i metode zaštite aplikacija. 2. Procijeniti ranjivosti i sigurnosne probleme u sklopu aplikacije. 3. Osmisliti način zaštite i smanjenja ranjivosti aplikacije. 4. Organizirati proces razvoja aplikacije sa željenom razinom sigurnosti. 5. Odabrati između više metoda i pristupa zaštite aplikacije Kolegij podržava i doprinosi sljedećim e-kompetencijama prema European e-Competence okviru: ● A.5. Architecture Design ● A.6. Application Design ● E.5. Process Improvement Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: ● GIAC Web application penetration tester ● GIAC Certified web application defender
a. Sadržaj predmeta	● Uvod u aplikacijsku sigurnost, problem proizvoljnog unosa u aplikaciju, modifikacija kontrole toka i "čudni strojevi" (eng. Weird Machines). Osnove DevSecOps principa. ● Sigurnosni propusti u aplikacijama fokusirani na stog i hrpu, propusti u baratanju ulazom i izlazom, Return-oriented programiranje, propusti u baratanju vremenom, propusti u konfiguraciji, sigurnosni problemi zbog krivog podešavanja sustava, implementacijske greške u primjeni kriptosustava, izlaganje i curenje osjetljivih podataka,. ● Metode zaštite aplikacija, zabrana izvršavanja (NX/W^X), provjera manipulacije na stogu i hrpi, randomizacija adresnog prostora, izolacija, odvajanje privilegija, kontejnerizacija, potpisivanje koda. ● Napadi na web aplikacije: OWASP top 10 klase napada umetanje znakova, problemi sa autentikacijom i upravljanje sesijama, Cross-Site Scripting (XSS), nesiguran direktni pristup objektima, nedostatak kontrole pristupa nad funkcijama, Cross Site Request

	Forgery (CSRF), korištenje poznatih ranjivih komponenata, neprovjerena usmjeravanja i preusmjeravanja. Napadi na web servise (SOAP, RESTful). ● Metode zaštite web aplikacija, filtiranje, separacija, sanitizacija, izolacija, primjena ESAPI-a, primjena aplikacijskih vatrozida. ● Napadi na poslužiteljske aplikacije i infrastrukturu: Napadi na sustave poruka (MQ) i autentikacijske sustave (SSO). Napadi na infrastrukturu računalnog oblaka i kontejnera. ● Organizacija sigurnog razvoja programskih proizvoda: recenziranje koda, programiranje u paru, automatizirano testiranje prije implementacije, norme za sigurni razvoj i testiranje, norme za verifikaciju razine sigurnosti.

b. Vrste izvođenja nastave:	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ on line u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)	c. Komentari: 30h predavanja i 100h samostalnog rada i učenja uz potporu e-učenja i mentorskog rada
d. Obveze studenata	Studenti preuzimaju i odrađuju samostalni problemski zadatak iz njihove odabrane domene tehničke ili organizacijske specijalizacije. Poželjno je da je domena problemskog zadatka iz područja rada tj. radnih obaveza kandidata. U terminu usmenog ispita kandidat uz klasični usmeni ispit brani projekt.		

e. Praćenje rada studenata									
	Pohađanje nastave	DA		Projekt			Pismeni ispit		
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		
	Kolokvij			Seminarski rad			(ostalo upisati)		
				Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)		

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Dowd, Mark, John McDonald, and Justin Schuh. The art of software security assessment: Identifying and preventing software vulnerabilities. Pearson Education, 2006.		
	Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd edition, Wiley, 2011.		
	Peter Yaworski. Real-World Bug Hunting: A Field Guide to Web Hacking. No Starch Press, 2019.		
	Andrew Hoffman. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly, 2020.		
	Liz Rice. Container Security: Fundamental Technology Concepts that Protect Containerized Application. O'Reilly, 2020.		

	Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea, Adam Stubblefield. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems, O'Reilly, 2020.		
2.11. Dopunska literatura (navesti naslov)	• Malcolm McDonald. Web Security for Developers: Real Threats, Practical Defense, No Starch Press; 2020. • Sanjib Sinha. Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities in Web sites and Applications, Apress, 2019. • Harpreet Singh, Himanshu Sharma. Hands-On Web Penetration Testing with Metasploit: The subtle art of using Metasploit 5.0 for web application exploitation. Packt Publishing, 2020. • Prema interesima polaznika, jer je vezana uz konkretnu tehnologiju ili programski jezik.		

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.3. Nositelj predmeta	Igor Tomičić	1.7. Godina studija	1
1.4. Naziv predmeta	Socijalni inženjering	1.8. Broj bodova po ECTS sustavu	5
1.4. Suradnici		1.9. Način izvođenja nastave (broj sati P + V + S + e-učenje)	20+0+10
1.5. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.10. Očekivani broj studenata na predmetu	10-15
1.6. Status predmeta	Izborni	1.11. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Temeljni cilj kolegija Socijalni inženjering je podizanje svijesti i znanja o ključnom utjecaju ljudskog faktora na sigurnost informacijskih sustava, kroz savladavanje znanstvenih temelja metoda koje se aktivno koriste u socijalnom inženjeringu. Takvi temelji i metode obuhvaćaju primijenjene komunikacijske modele, kontekstno profiliranje, metode i principe utjecaja i manipulacije, lažiranje identiteta, stvaranje umjetnog konteksta, identifikaciju napada, OSINT (eng. *open source intelligence*) metode, tehnike i alate, fizičku sigurnost, itd. Razumijevanjem principa socijalnog inženjerstva, studenti će moći identificirati i klasificirati napade, te koristiti naučene metode unutar procesa penetracijskog testiranja i/ili procesa crvenih timova u testiranju sustava informacijske sigurnosti, imajući u vidu etičke i zakonske okvire unutar kojih djeluju.		
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata sigurnosti informacijskih sustava.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/informacijskom sustavu.		

<table>
<tr><td></td><td colspan="3">2. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava.
3. Uspostaviti i provoditi učinkovit trening za podizanje znanja i svijesti o informacijskoj sigurnosti s ciljem provođenja usvojenih sigurnosnih politika i procedura
4. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike.</td></tr>
<tr><td>a. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)</td><td colspan="3">1. Razviti strategiju napada na ciljani sustav koristeći principe i metode socijalnog inženjerstva
2. Stvoriti procedure i politike organizacije za prevenciju utjecaja metoda socijalnog inženjeringa
3. Stvoriti kontingencijske planove u slučaju proboja informacijskog sustava tehnikama socijalnog inženjeringa
4. Vrednovati razinu svijesti i pripremljenosti organizacije za napade socijalnim inženjeringom
5. Preporučiti metode i tehnike te integraciju socijalnog inženjerstva u proces penetracijskog testiranja</td></tr>
<tr><td>b. Sadržaj predmeta</td><td colspan="3">Uvod u Socijalni inženjering. Studije primjera za motivaciju.
Metode i tehnike napada socijalnim inženjeringom; analize ljudskih ranjivosti.
Znanstveni principi odabranih funkcija ljudskog mozga (amigdala, procesiranje informacija, utjecaj emocija).
Profiliranje, komunikacijski stilovi, primijenjena neverbalna komunikacija.
Principi i tehnike utjecaja, manipulacije i elicitacije.
Principi „pretextinga“, studije slučajeva, metode izrade umjetnog konteksta.
Sakupljanje informacija (OSINT), alati, tehnike. Priprema računala za OSINT proces; pregled potrebnih tehnologija. Napredno korištenje internetskih tražilica. Pregled socijalnih mreža i online zajednica.
Pretraživanje i analiza email adresa, korisničkih imena, telefonskih brojeva, domenskih imena, IP adresa, dokumenata, fotografija, i ostalih izvora slobodno dostupnih informacija.
Sinteza metodologije penetracijskog testiranja.
Procedure i politike organizacije za prevenciju utjecaja metoda socijalnog inženjeringa te kontingencijski planovi u scenariju proboja informacijskog sustava tehnikama socijalnog inženjeringa.
Dokumentiranje, izvještavanje, zakonski okviri.</td></tr>
<tr><td>c. Vrste izvođenja nastave:</td><td>☒ predavanja
☒ seminari i radionice
☐ vježbe
☐ on line u cijelosti
☒ mješovito e-učenje
☐ terenska nastava</td><td>☒ samostalni zadaci
☐ multimedija i mreža
☐ laboratorij
☒ mentorski rad
☐ (ostalo upisati)</td><td>d. Komentari:</td></tr>
<tr><td>e. Obveze studenata</td><td colspan="3">Projekt: izrada i izvršenje plana penetracijskog testiranja u kontekstu socijalnog inženjeringa nad legalnim ciljevima</td></tr>
</table>

f. Praćenje rada studenata	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit	DA	NE	
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	NE	
	Esej			Referat			(ostalo upisati)	DA	NE	
	Kolokvij			Seminarski rad			(ostalo upisati)	DA	NE	
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**		

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Hadnagy, C. (2018). *Social engineering: The science of human hacking*. John Wiley & Sons.		DA
	Cialdini, R. B. (2006). Influence: the psychology of persuasion, revised edition. *New York: William Morrow*.		DA
	Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform.		DA
2.11. Dopunska literatura (navesti naslov)	• Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.		

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Petra Grd	1.6. Godina studija	1
1.2. Naziv predmeta	**Sustavi fizičke i logičke kontrole pristupa**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici		1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	15+0+15+0
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	2. razina, 10%

2. OPIS PREDMETA	
2.1. Ciljevi predmeta	Temeljni cilj kolegija jest naučiti polaznike o sustavima kontrole pristupa, načinima kontrole pristupa te kako implementirati sustave kontrole pristupa. Realizira se kroz: analizu najčešćih načina prodora u informacijske sustave kao i oblika zlouporabe informacija/podataka (iz oblika zlouporabe informacija/podataka mora se odrediti tip ranjivost kao i moguća protumjera), primjenu metoda kontrole pristupa, kontrolu i reviziju učinjenih aktivnosti, analizu i prepoznavanje potrebnih mjera za kvalitetnu kontrolu pristupa i smanjenje mogućih šteta, predlaganje i prezentaciju sustava kontrole pristupa u poslovnim/informacijskim sustavima, vrednovanje izvedenih aktivnost tijekom realizacije kolegija.
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu 2. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti 3. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 4. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike. 5. Analizirati, procijeniti i unaprijediti odgovarajuća tehnološka rješenja u uspostavi sustava informacijske sigurnosti. 6. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera.
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	Očekivani ishodi učenja: 1. Analizirati najčešće načine prodora u informacijske sustave kao i oblika zlouporabe informacija/podataka. 2. Povezati zlouporabe informacija/podataka, tipove ranjivosti koje iskorištavaju i moguće mjere zaštite. 3. Preporučiti sustav kontrole pristupa u poslovnim/informacijskim sustavima. 4. Vrednovati implementirani sustav kontrole pristupa. Kolegij je razvijen u skladu sa znanjima i vještinama propisanim Europskim kvalifikacijskim okvirom.

	• K1 utjecaj pravnih propisa na informacijsku sigurnost • K2 moguće sigurnosne prijetnje • S1 definirati, prezentirati i promovirati politiku informacijske sigurnosti višem menadžmentu organizacije • S2 primijeniti relevantne standarde, najbolje prakse i pravne propise za informacijsku sigurnost • S3 predvidjeti potrebne promjene u strategiji informacijske sigurnosti organizacije i formulirati nove planove Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: • (ISC)2 SSCP – Systems Security Certified Practitioner • (ISC)2 CISSP – Certified Information Systems Security Professional
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Uvod u predmet. Kontrola pristupa. Razlike fizičke i logičke kontrole pristupa. Zakonska regulativa. Autentifikacija i identifikacija. Fizička kontrola pristupa. Načini fizičke kontrole pristupa. Logička kontrola pristupa. Alati i protokoli. Operacijski sustavi, aplikacije, baze podataka. Kombinacija logičke i fizičke kontrole pristupa. Definicija biometrije i osnovne podjele. Metode identifikacije kroz razvoj informacijske tehnologije. Pregled najčešće korištenih biometrijskih karakteristika. Osnovna i posebna zakonska regulativa proizvodnje i korištenja biometrijskih uređaja. Zakonska regulativa korištenja biometrijskih karakteristika. Biometrijski uzorak i arhitektura biometrijskog sustava. Prikupljanje i procesiranje biometrijskog uzorka. Prepoznavanje i identifikacija. Temeljni opis psiholoških karakteristika. Specifičnosti i ograničenja psiholoških karakteristika. Primjenjivost fizičkih biometrijskih karakteristika. Metode i alati za uzimanje uzoraka. Sustavi za verifikaciju i identifikaciju slika otisaka prsta. Sustavi za predprocesiranje, procesiranje, procesiranje i prepoznavanje slika otisaka prsta. Uvjeti i metode izuzimanja geometrije dlana kao biometrijskog uzorka. Evaluacija izvođenja potpisa, biometrijske karakteristike. Osnovni koncept potpisa i njegova biometrijska obilježja. Algoritam za usporedbu potpisa. Uzorak šarenice kao biometrijska karakteristika. Tehnologija koja koristi mrežnicu kao osnovnu biometrijsku karakteristiku. Izgradnja biometrijskog modela baziranog na uhu i njegove osnovne karakteristike. Forenzika DNA. Načini izuzimanja i usporedbe DNA. Psihološka sposobnost prepoznavanja lica. Načini izuzimanja i izlučivanja karakteristika. Metode opisa lica. Sustavi detekcije i identifikacije. Procesiranje govora i glasa u kontekstu biometrijskih karakteristika. Izlučivanje i selekcija karakteristika. Principi termogramske identifikacije. Razlike između termograma lica i termograma tijela. Osnovni elementi biometrijskog sustava baziranog na dinamici tipkanja. Osnovne karakteristike biometrijskog sustava baziranog na hodu. Osnovni elementi biometrijskog sustava baziranog na mirisu. Otisak jezika.

	Pouzdanost sustava. Mogućnosti varanja biometrijskih čitača. Manipulacije sigurnosnim sustavima. Manipulacije pri izgradnji sigurnosnih sustava i propusti u izgradnji. Izgradnja biometrijske smart kartice. Implementacija biometrijskih karakteristika u profesionalnu i specifičnu strojnu podršku. Implementacija biometrijskih karakteristika u strojnu podršku opće namjene.

2.6. Vrste izvođenja nastave:			2.7. Komentari:
	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ *on line* u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)	

2.8. Obveze studenata	Studenti preuzimaju i odrađuju samostalni problemski zadatak iz njihove odabrane domene tehničke ili organizacijske specijalizacije. Poželjno je da je domena problemskog zadatka iz područja rada tj. radnih obaveza kandidata. U terminu usmenog ispita kandidat uz klasični usmeni ispit brani projekt.

2.9. Praćenje rada studenata									
	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		NE
	Eksperimentalni rad	DA		Istraživanje	DA		Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		NE
	Kolokvij			Seminarski rad			(ostalo upisati)		NE
				Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)	**5**	

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Mike Chapple, Bill Ballad, Tricia Ballad, Erin Banks: Access Control, Authentication, and Public Key Infrastructure: Print Bundle (Jones & Bartlett Learning Information Systems Security) 2nd Edition, 2013.	1	
	Bolle, R., Connell, J., Pankanti, S., Ratha, N., Senior, A., Guide to Biometrics (Springer Professional Computing), Springer-Verlag, 2003.	1	
	Julian Ashbourn: Practical Biometrics: From Aspiration to Implementation, Springer; 2nd ed. 2015 Edition.	1	

2.11. Dopunska literatura (navesti naslov)	• Ashbourn, J., Biometrics: Advanced Identify Verification: The Complete Guide, Springer-Verlag, 2000. • Castleman, K. R., Digital Image Processing, Prentice Hall • Reid, P. Biometrics and Network Security, Prentice Hall PRT, Upper Saddle River, New Jersey, 2004 • Woodward, J., Orlans, N.M., Higgins, P.T., Biometircs, McGraw-Hill Osborne, 2000. • Zhang, D., Jing, X., Yang, J., Biometric Image Discrimination Technologies, Idea Group Publishing, 2006.

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Igor Tomičić Nikola Ivković	1.6. Godina studija	1
1.2. Naziv predmeta	**Testiranje sustava sigurnosti i etičko hakiranje**	1.7. Bodovna vrijednost (ECTS)	5
1.3. Suradnici		1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20 + 10
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	2, 10%

2. OPIS PREDMETA	
2.1. Ciljevi predmeta	Naučiti polaznike metode i načine provjere razine sigurnosti složenih sustava. Prikazati metodologije za testiranje razine sustava sigurnosti.
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu 2. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava. 3. Analizirati, preporučiti i odabrati sigurnosne zahtjeve prilikom dizajna, razvoja i uspostave sustava informacijske sigurnosti 4. Analizirati resurse informacijskog sustava s aspekta njihove ranjivosti i sigurnosnih nedostataka. 5. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 6. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Evaluirati primjenu raznih metodologija i pristupa testiranju sustava sigurnosti. 2. Odabrati primjerenu metodologiju i pristup testiranju sustava sigurnosti prema konkretnom zahtjevu i opsegu testiranja. 3. Kritički prosuđivati etičke principe, pravnu regulativu i znati moguće rizike u sklopu testiranja sustava sigurnosti i etičkog hakiranja. 4. Organizirati pristup i način testiranja sustava sigurnosti za odabrani sustav. 5. Preispitati odabrane metode testiranja sigurnosti. 6. Evaluirati i procijeniti razinu sigurnosti u sustavu primjenom metodologije. Kolegij podržava i doprinosi sljedećim e-kompetencijama prema European e-Competence okviru: • B.3. Testing

	• E.3. Risk Management • E.5. Process Improvement • E.6. ICT Quality Management Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: • EC Council Certified Ethical Hacker • GIAC Systems and Network Auditor • GIAC Penetration tester		
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Uvod u predmet: objašnjenje metode rada na kolegiju, odabir tema za problemske zadatke. Etička i pravna pitanja u području testiranja sustava sigurnosti i etičkog hakiranja. Zakonska regulativa i moguća kaznena odgovornost. Razine provjere sustava sigurnosti, skeniranje za ranjivostima, penetracijski testovi, revizije sustava, testiranje Pristupi testiranju sustava sigurnosti, određivanje i dokumentiranje opsega testiranja, potrebni dokumenti i dozvole prije testiranja, pisanje izvješća testiranja. Metodologije testiranja sustava sigurnosti i odabir primjerene metodologije ovisno o specifičnostima sustava koji se testira. Osnove OSSTMM metodologije (eng. The Open Source1 Security Testing Methodology Manual). Testiranje razine svijesti osoblja o sigurnosti, razina prijevara i izloženosti socijalnom inženjeringu, sigurnosti računalne i telekomunikacijske mreže, bežičnih uređaja, mobilnih uređaja, fizičke sigurnosne kontrole pristupa, sigurnosnih procesa te sigurnosti fizičke lokacije. Koraci u testiranju i etičkom hakiranju, postupci prije testiranja, izviđanje, modeliranje prijetnji, analiza ranjivosti, eksploatacija, post-eksploatacija, izvješćivanje. Priprema za penetracijsko testiranje Odabir meta na temelju procjene rizika. Vrste penetracijskih testova. Odabir opsega za penetracijsko testiranje. Prednosti i mane izgradnje internog tima za penetracijsko testiranje. Aktivnosti poslije penetracijskog testiranja Razumijevanje izvješća penetracijskog testa, postupanje s rezultatima penetracijskog testa i smanjenje uočenih ranjivosti, ponovni test. Načini realiziranja metodologije testiranja kroz konkretne metode testiranja - Prikaz metoda testiranja ovisi o interesu i specijalizaciji polaznika		
	☒ predavanja	☒ samostalni zadaci	2.7. Komentari:

2.6. Vrste izvođenja nastave:	☒ seminari i radionice ☐ vježbe ☐ *on line* u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)	30h nastavnih sadržaja i 100h samostalnog rada i učenja uz potporu e-učenja i mentorskog rada

2.8. Obveze studenata	Vježba: pripremiti projekt vanjskog penetracijskog testiranja na primjeru organizacije.								
2.9. Praćenje rada studenata	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		
	Kolokvij			Seminarski rad			(ostalo upisati)		
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**5**	

2.11. Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	**Naslov**	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**
	Hickey, M., Arcuri, J. (2020) Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming		
	Stouffer, K., Falco, J., & Scarfone, K. (2008). NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology (September, 2008).		Neograničeno
	Herzog, Pete: Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/research/osstmm.html		Neograničeno
	Weidman, Georgia. Penetration Testing: A Hands-on Introduction to Hacking. No Starch Press, 2014.		Neograničeno
	Penetration testing execution standard (http://www.pentest-standard.org/index.php/Main_Page)		Neograničeno

2.12. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)	• OWASP Testing Project: https://www.owasp.org/index.php/OWASP_Testing_Project

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Željko Hutinski Mario Spremić	1.6. Godina studija	1
1.2. Naziv predmeta	**Upravljanje informacijskom sigurnošću**	1.7. Broj bodova po ECTS sustavu	6

1.3. Suradnici	Renata Mekovec	1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	20 + 0 +10
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Obavezni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2 ,10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Temeljni cilj kolegija jest naučiti polaznike kako uspostaviti cjeloviti sustav informacijske sigurnosti i upravljati sustavom informacijske sigurnosti. Način uspostave i upravljanja sustavom sigurnosti temelji se na poznavanju šire problematike informacijske sigurnosti i izgradnji sustava sigurnosti temeljenog na najboljoj praksi međunarodnog skupa normi ISO 27000 i NIST 800.		
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Definirati, osmisliti i primijeniti strategiju uspostave sustava informacijske sigurnosti 3. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava 4. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti. 5. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture. 6. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava, zaposlenici, klijenti, institucije državne uprave).		
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Razumjeti i analizirati značaj cjelovitog sustava informacijske sigurnosti. Time se određuje i oslonjivost poslovnog sustava na informacijski sustav, 2. Poznavati i primijeniti metode i norme za uspostavu cjelovitih sustava informacijske sigurnosti te upravljanja procjenom značaja informacijske imovine, procjenom oblika i intenziteta prijetnji te procjenom rizika, 3. Analizirati i prepoznati informacijsku imovinu, sigurnosne prijetnje i druge čimbenike nužne za procjenu ranjivosti informacijskog sustava i poduzimanje potrebnih mjera za smanjivanje ranjivosti, 4. Predložiti i osmisliti program razvoja i uvođenja sustava informacijske sigurnosti u poslovni sustav i voditi takav projekt do njegove certifikacije Kolegij podržava sljedeće e-kompetencije prema European e-Competence okviru: ● D.1. Information Security Strategy Development		

	● E.8. Information Security Management Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: ● ISACA CISM Certified Information Security Manager ● ISACA CGEIT Certified in the Governance of Enterprise IT ● (ISC)^2 CISSP Certified Information Systems Security Professional
2.5. Sadržaj predmeta	Uvod u predmet: objašnjenje metode rada na kolegiju, podjela korisničkih računa za pristup LMS-u (Moodle) na kojem se nalazi nastavni sadržaj preko kojeg se koriste alati za diskusijske skupine, odabir tema za projektne radove te predaja radova u korisničkom okruženju. Razlozi izgradnje sustava informacijske sigurnosti: Oslonjenost poslovnog sustava na informacijski sustav, principi podjele informacija u zajedničkim informacijskim sustavima. Pregledi stanja ovog područja u svijetu i RH. Ciljevi sigurnosti IS-a. Mogući aspekti i razine sigurnosti IS-a. Pregled normi (standarda) iz ovog područja. Načini, aspekti i parametri organizacijske sigurnosti IS-a. Pridobivanje potpore poslovodstva. Koraci izgradnje sustava sigurnosti prema skupu normi ISO/IEC 27000, NIST 800. Definiranje politika informacijske sigurnosti, upravljanje informacijskom imovinom, procjene sigurnosnih rizika, pregled kvalitativnih i kvantitativnih metoda procjene rizika, odabir odgovarajućih kontrola. Upravljanje sigurnosnim rizicima u malim i srednjim poslovnim sustavima. Pristupi u korporacijskim sustavima. Uloga voditelja informacijske sigurnosti (tzv. CISO, Chief Information Security Officer). Prezentiranje i komunikacija prema upravi organizacije i upravnom/nadzornom odboru. Podizanje svijesti o informacijskoj sigurnosti. Odabir mjera za smanjenje rizika i obrada rizika. Upravljanje razvojem sustava sigurnosti. Prikaz načina izrade bilance informacijske imovine, procjene značaja podatkovnog sadržaja. Upravljanje izradom procjene izvora, oblika i intenziteta prijetnji. Mjere za smanjivanje rizika: otpornost pojedinog materijalnog nositelja prema oblicima prijetnji. Programske mjere zaštite informacijskog sustava. Tehničke mjere zaštite informacijskog sustava. Fizičke mjere zaštite informacijskog sustava. Organizacijske mjere zaštite informacijskog sustava. Pravne i druge normativne mjere zaštite informacijskog sustava. Propisi Europske zajednice i NATO-a iz područja sigurnosti informacija, Nacionalni program informacijske sigurnosti Republike Hrvatske. Hrvatsko zakonodavstvo iz ovog područja. Upravljanje razvojem cjelovitog sustava informacijske sigurnosti. Organizacija projekta i sudionici. Određivanje područja primjene, izrada plana projekta, proizvodi i usluge po fazama projekta. Organizacijska struktura za upravljanje informacijskom sigurnošću. Nadzor tijekom realizacije projekta. Certifikacija sustava informacijske sigurnosti.

2.6. Vrste izvođenja nastave:	☒ predavanja ☐ seminari i radionice ☐ vježbe ☐ on line u cijelosti ☒ mješovito e-učenje ☐ terenska nastava		☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☒ studije slučaja			2.7. Komentari 30 h nastave + 130h samostalnog rada i učenja uz potporu e-učenja i mentorskog rada			
2.8. Obveze studenata	Studenti preuzimaju i odrađuju samostalni problemski zadatak iz njihove odabrane domene tehničke ili organizacijske specijalizacije. Poželjno je da je domena problemskog zadatka iz područja rada tj. radnih obaveza kandidata. U terminu usmenog ispita kandidat uz klasični usmeni ispit brani projekt. Izraditi plan projekta sustava upravljanja informacijskom sigurnošću na primjeru organizacije s očekivanim aktivnostima, njihovim nosiocima i ishodima projekta								
2.9. Praćenje rada studenata	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		NE
	Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
	Esej			Referat			(ostalo upisati)		NE
	Kolokvij			Seminarski rad			(ostalo upisati)		NE
				Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**6**	

2.10. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
	Krakar, Z; Tomić Rotim, S; Žgela, M; Arbanas, K; Kišasondi, T: Korporativna informacijska sigurnost; Fakultet organizacije i informatike, 2014, Varaždin	5	
	Calder, A: IT governance : a manager's guide to data security and ISO 27001/ISO 27002		Neograničena
	ISO/IEC 27002:2013: Information technology, Security techniques: Code of practice for information security controls		Neograničeno
	ISO/IEC 27001:2013: Information technology, Security techniques: Information Security Management Systems, Requirements.		Neograničena
	National Institute of Standards and Technology: Special Publication series 800 and 1800 (http://csrc.nist.gov/publications/PubsSPs.html)		Neograničena
	ISACA Business Model for Information Security		
	ISACA Official CISM review manual		
	(ISC)^2 Official Guide to the CISSP CBK Reference 5th Edition		

2.11. Dopunska literatura (navesti naslov)	Dopunska literatura definira se kroz mentorski rad sa polaznikom i vezana je uz konkretnu domenu specijalizacije polaznika.

1. OPĆE INFORMACIJE

1.1. Nositelj predmeta	Petra Grd Igor Tomičić	1.6. Godina studija	1
1.2. Naziv predmeta	**Upravljanje incidentima i računalna forenzika**	1.7. Bodovna vrijednost (ECTS)	6
1.3. Suradnici		1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20+0+10+0
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Obavezan	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta *on line* (maks. 20%)	2. razina, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Temeljni cilj kolegija jest naučiti polaznike kako upravljati incidentima i koristiti procedure računalne forenzike za prikupljanje i analizu digitalnih dokaza. Realizira se kroz: primjenu upravljanja incidentima, analizu koraka koji poduzimaju napadači kod napada na sustav, predlaganje koraka za sprječavanje napadača u daljnjim napadima na sustav, primjenu računalne forenzike i procedura za provedbu računalne forenzike, razlikovanje stalnih i nestalnih podataka i njihove važnosti za računalnu forenziku, forenzičko prikupljanje relevantnih digitalnih dokaza i rukovanje digitalnim dokazima bez ugrožavanja njihovog integriteta, analizu podataka i rekonstrukciju događaja sa Windows i Linux operacijskih sustava te kreiranju forenzičkog nalaza i mišljenja.		
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Analizirati, razviti, primijeniti i vrednovati metode i načine zaštite resursa informacijskog sustava s ciljem sprečavanja narušavanja njegova integriteta, detekcije neovlaštenih aktivnosti i napada, te uspostave odgovarajućih zaštitnih mjera. 3. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti. 4. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture 5. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava, zaposlenici, klijenti, institucije državne uprave).		
2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	Polaznici će biti u stanju: 1. Primijeniti metode upravljanje incidentima 2. Analizirati korake koje poduzimaju napadači kod napada na sustav 3. Predložiti korake za sprječavanje napadača u daljnjim napadima na sustav u okviru studije slučaja 4. Primijeniti procedure računalne forenzike. 5. Forenzički prikupiti relevantne digitalne dokaze i rukovati digitalnim dokazima bez ugrožavanja njihovog integriteta 6. Analizirati podatke i rekonstruirati događaje s Windows i Linux operacijskih sustava		

	7. Kreirati forenzički nalaz i mišljenje Kolegij je razvijen u skladu sa znanjima i vještinama propisanim Europskim kvalifikacijskim okvirom. • K1 tehnike detekcije sigurnosti, uključujući mobilne i digitalne • K2 tehnike cyber napada i protumjere za njihovo izbjegavanje • K3 računalna forenzika • S1 primijeniti tehnike nadzora i testiranja • S2 uspostaviti plan oporavka • S3 implementirati plan oporavka u slučaju krize Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: • ISACA CISA Certified Information Systems Auditor
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	Proces upravljanja incidentima Definicija prema ITIL. Aktivnosti ICM-a. Rukovanje incidentom. Rješavanje i oporavak. Sprečavanje daljnje štete. Završavanje incidenta. Izvještavanje. Prikrivanje tragova od strane napadača Mogući tragovi. Prikrivanje datoteka i direktorija na Windows i Linux operacijskim sustavima. Prikrivanje tragova Osnove digitalne forenzike Povijest forenzike. Forenzika računala u današnjem svijetu. Proces provedbe forenzike računala. Rukovanje s incidentima. Izvješće o napretku. Etika. Tipovi tehnologija za forenziku računala. Vojne, poslovne i specijalizirane tehnike. Enkripcijske metode. Tipovi sustava za forenziku računala. Internet security systems. Intrusion Detection systems, Firewall security systems. Usluge, istraživački servisi, digitalni detektiv, slučajevi. Razumijevanje provedbe pretrage/istrage računala Locardov trokut. Načini izvršenja. Metodologije, definiranje i opis digitalnog dokaza za potrebe suda. Digitalni dokazi Definicija digitalnog dokaza, digitalni lanac dokaza. Prikupljanje dokaza i njihovo izuzimanje, pravila dokaza, metode prikupljanjem aritifakti, rekonstrukcija događaja. Stalni i nestalni digitalni dokazi, definiranje i opis digitalnog dokaza u poslovnom okruženju. Prikupljanje digitalnih dokaza, priprema i očuvanje dokaza Forenzički povrat podataka Algoritmi, metodologija. Razlike između komercijalnih i open source rješenja, razlike između forenzičkih i „klasičnih“ načina povrata podataka Struktura i analiza datotečnih sustava Windows datotečni sustav. Linux datotečni sustav. Identificiranje, prikupljanje i analiza dokaza s bilo kojeg sloja datotečnog sustava. Artefakti operacijskog sustava. Sigurnosna kopija sustava Analiza datoteka i aktivnosti programa

	Windows registra. Metapodaci datoteka. Artefakti datotečnih sustava. Analiza logova. Analiza komunikacije korisnika Host-based email aplikacije. Mobilne e-mail aplikacije. Instant messaging. Ostale aplikacije za komunikaciju Promjenjivi podaci Normalna i sumnjiva aktivnost unutar promjenjive memorije. Identifikacija zlonamjernih procesa, mrežnih konekcija, sistemskih podataka. Način i vrijeme prikupljanja promjenjivih podataka. Očuvanje integriteta i dokumentiranje promjenjivih podataka. Osnove mrežne forenzike Mrežna forenzika, Hvatanje mrežnog prometa, Drugi dokazi na mreži, TCP zaglavlje, Primjena Snort-a, komercijalne NetFlow aplikacije, NetWithness, SilentRunner, inkomporiranje mrežne forenzike u plan djelovanja u slučaju incidenta Forenzika malwarea Prikupljanje nestalnih podataka u Windows okruženju, prikupljanje nestalnih podataka u Linux okruženju, prikupljanje podataka na živim sustavima, prikupljanje podataka na postmortem sustavima, otkrivanje i ekstrakcija malwarea, identifikacija datoteka, analiza sumnjivih aplikacija Forenzički laboratorij Načini izgradnje forenzičkog laboratorija. Sustav za upravljanjem i pohranom digitalnih dokaza. Analiza i standardizacija forenzičke opreme. Komercijalni forenzički alati, EnCase, FTK. Open source forenzički alati. Izrada forenzičkog nalaza i mišljenja Načini pisanja i generiranje izvještaja, priprema izvještaja za poslovodstvo. Načini pisanja i generiranja izvještaja za sud. Priprema prezentacije, način prezentiranja u poslovnom okruženju i u sudnici.
2.6. Vrste izvođenja nastave:	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ *on line* u cijelosti ☒ mješovito e-učenje ☐ terenska nastava ☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati) 2.7. Komentari:
2.8. Obveze studenata	Studenti preuzimaju i odrađuju samostalni problemski zadatak iz njihove odabrane domene tehničke ili organizacijske specijalizacije. Poželjno je da je domena problemskog zadatka iz područja rada tj. radnih obaveza kandidata. U terminu usmenog ispita kandidat uz klasični usmeni ispit brani projekt.

2.9. Praćenje rada studenata									
	Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		NE
	Eksperimentalni rad		NE	Istraživanje	DA		Usmeni ispit	DA	
	Esej		NE	Referat		NE	(ostalo upisati)		NE
	Kolokvij		NE	Seminarski rad		NE	(ostalo upisati)		NE
			NE	Praktični rad	DA		Broj bodova po ECTS sustavu (ukupno)	**6**	

2.10. Dopunska literatura (navesti naslov)	**Naslov**	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**

	Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition, Packt Publishing, 2020.	1	
	Leighton Johnson: Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response, Elsevier Inc, 2014.	1	
	John Sammons: The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Elsevier Inc, 2012.	1	
	Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents, Packt Publishing, 2017.	1	
2.11. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)	• Marie-Helen Maras: Computer Forensics: Cybercriminals, Laws, and Evidence, Jones and Bartlett Learning LLC, 2015. • Darren R. Hayes: A Practical Guide to Computer Forensics Investigations, Pearson Education, 2015.		

1. OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Mario Žgela Valentina Kirinić	1.6. Godina studija	1
1.2. Naziv predmeta	**Upravljanje kontinuitetom poslovanja**	1.7. Bodovna vrijednost (ECTS)	6
1.3. Suradnici	Biljana Cerin	1.8. Način izvođenja nastave (broj sati P+V+S+e-učenje)	20 + 0 + 10
1.4. Studijski program (preddiplomski, diplomski, integrirani)	Poslijediplomski specijalistički studij	1.9. Očekivani broj studenata na predmetu	10-15
1.5. Status predmeta	Izborni	1.10. Razina primjene e-učenja (1, 2, 3 razina), postotak izvođenja predmeta on line (maks. 20%)	2, 10%
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	Ciljevi i sadržaj predmeta izrađeni su i usklađeni s European e-Competence Framework, V.3.0. Temeljni cilj predmeta je upoznati polaznike s potrebom uspostave sustava upravljanja kontinuitetom poslovanja (Business Continuity Management System – BCMS) i njegovom ICT komponentom, naučiti ih pripremiti takve poduhvate, koristiti norme		

	(standarde) i metode njegovog razvoja, načine implementacije, primjene i provjere takvih sustava. Realizira se kroz slijedeće podciljeve i logičke cjeline: • razumijevanje značaja uspostave BCMS-a, prepoznavanje opasnosti od prekida poslovanja, osobito ključnih poslovnih procesa i ICT potpore, na poslovanje tvrtke, • upoznavanje s različitim pristupima uspostavi BCM sustava (DRI, BCI, BSI, ISO i dr.) i prepoznavanje životnog ciklusa takvih sustava • upoznavanje s načinima razvoja pojedinih faza BCMS-a • BIA analize (Business Impact Analysis), upravljanja BCM rizicima, oblikovanja strategije BCMS-a, izrade planova BCMS-a, uvježbavanja BCMS-a, procjenjivanja i testiranja BCMS-a i razvoja kulture BCMS-a, • upoznavanje s načinom razvoja BCMS-a u skladu s njegovim životnim ciklusom, osobito primjenom norme ISO/IEC 22301, upoznavanje s ICT potporom takvim sustavima – procjenom spremnosti ICT-a za BCM, određivanjem kritičnih ICT resursa, procjenama rizika ICT potpore, izradom ICT strategije za BCMS, strukturiranjem i arhitekturom ICT opreme za BCMS, • upoznavanje s načinom razvoja zrelosti BCMS-a, razvojem kompetencija za takve sustave, osobnim certifikacijama u ovom području i certifikacijom cjelokupnog sustava i • upoznavanje s praksom i primjenom BCMS-a, naročito podržanih suvremenim informacijsko – komunikacijskim tehnologijama. Stečeno metodološko znanje primjenjuje se u radionicama u kojima se rješavaju pojedina specijalistička pitanja i izabiru najbolja BCMS rješenja .
2.2. Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti. Znanja i vještine usvojeni završetkom diplomskog studija.
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Definirati, osmisliti i primijeniti strategiju uspostave sustava informacijske sigurnosti. 3. Uspostaviti i primijeniti planove i procedure za osiguranje informacijske imovine, uključujući i planove oporavka, u skladu s međunarodnim normama, zakonskim aktima i iskustvima dobre prakse. 4. Ustrojiti i provoditi provjere sustava informacijske sigurnosti (audite) upotrebom odgovarajućih metoda i postupaka, s ciljem osiguravanja sukladnosti sustava informacijske sigurnosti sa sigurnosnim planovima i procedurama, politikama, međunarodnim standardima, zakonskim i internim aktima poslovnog sustava. 5. Uspostaviti i provoditi učinkovit trening za podizanje znanja i svijesti o informacijskoj sigurnosti s ciljem provođenja usvojenih sigurnosnih politika i procedura. 6. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti. 7. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture. 8. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava, zaposlenici, klijenti, institucije državne uprave).

2.4. Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Razumijevati i analizirati značaj uspostave sustava upravljanja kontinuitetom poslovanja, 2. Poznavati i primijeniti metode i prakse inicijalizacije poduhvata upravljanja kontinuitetom poslovanja, identifikacije ključnih poslovnih procesa, događaja koji mogu prekinuti poslovne procese, načina izrade i implementacije takvih planova, kao i njihovog testiranja 3. Prepoznati opasnosti od posljedica prekida poslovanja, necjelovitih rješenja, nedovoljne izobrazbe poslovodstva i vlasnika poslovnih procesa 4. Analizirati primjere iz prakse primjenom BCMS-a, naročito podržanih suvremenim informacijsko – komunikacijskim tehnologijama. Kolegij podržava sljedeće e-kompetencije prema European e-Competence okviru: • A2 K6 ICT standardi informacijske sigurnosti • D1 K2 Utjecaj zakonskih uvjeta na informacijsku sigurnost • E3 K1 Primijeniti metode procjene rizika uzimajući u obzir organizacijske vrijednosti i interese • E8 K3 Kritični rizici u upravljanju informacijskom sigurnošću • A2 S5 Predvidjeti i smanjiti ranjivosti od potencijalnih uzroka prekida poslovanja • D1 S4 Predvidjeti potrebne promjene u organizaciji te izraditi planove u cilju poboljšanja informacijske sigurnosti • E8 S2 Analizirati kritičnu imovinu tvrtke i prepoznati prijetnje i ranjivosti • E8 S7 Provoditi plan oporavka sustava u slučaju kriznog stanja Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima: • DRII CBCP Certified Business Continuity Professional
2.5. Sadržaj predmeta detaljno razrađen prema satnici nastave	1. Analiza poslovanja sa stajališta BCMS-a, prepoznavanje opasnosti od prekida poslovanja, osobito ključnih poslovnih procesa i prekida ICT potpore na poslovanje tvrtke. Potreba i značaj BCMS-a. Pravna regulativa koja nalaže nužnost uspostave BCM sustava – pregled međunarodnih i hrvatski propisa. Potencijalne opasnosti koje mogu dovesti do prekida u poslovnim procesima. Moguću učinci takvih prekida. ICT kao izvor rizika u BCMS-u. (5 sati) 2. Iniciranje projekta uspostave BCMS-a, upoznavanje s različitim pristupima uspostavi BCM sustava: DRI (Disaster Recovery Institute) , BCI (Business Continuity Institute) pristupom, normom BSI 100-4, normom ISO/IEC 22301, ITIL pristupom, COBIT pristupom i dr. Prepoznavanje životnog ciklusa BCMS-a: Razumijevanje vlastitog poslovanja, Strategija BCMS-a, Planovi neprekinutosti poslovanja, Usporedba mogućih pristupa i odabir optimalnog. (5 sati) 3. Razvoj pojedinih faza BCMS-a: BIA analize (Business Impact Analysis), upravljanja BCM rizicima prema nekoj od relevantnih metoda ili normi (preferira se ISO/IEC 31000), oblikovanja strategije BCMS-a, izrade planova BCMS-a, uvježbavanja BCMS-a, procjenjivanja i testiranja BCMS-a i razvoja kulture BCMS-a. (5 sati)

<table>
<tr><td></td><td colspan="6">4. Implementacija BCMS-a u skladu s njegovim životnim ciklusom, osobito primjenom norme ISO/IEC 22301. PDCA (Plan – Do – Check – Act) ciklus. Iniciranje BCM projekta, istraživanje potreba poslovnog sustava za BCM-om, određivanje područja primjene, određivanje politike kontinuiteta poslovanja, BIA, procjene rizika, razmatranje mogućih BC strategija, uloga računarstva u oblaku u kreiranju BC strategije. (2 sata)

5. Uspostava organizacijskog ustroja, izrada planova kontinuiteta, uspostava komunikacijskih kanala, treninzi i osvješćivanje, testiranje BCMS-a, nadzor, mjerenja i evaluacija BCMS-a, interni auditi BCMS-a, postupanje s nesukladnostima, kontinuirana unapređenja BCMS-a. (5 sati)

6. Održavanje i provjere BCMS-a: testiranje različitih scenarija, simulacija događaja, testiranje mogućnosti usluga i dobavljača, tehničko testiranje, testiranje oporavka na rezervnoj lokaciji, uvježbavanje BCM planova. (3 sata)

7. Programska oprema i ICT potpora BCMS-u. Analiza raspoložive programske opreme koja se koristi za BCMS, primjeri i analize situacija iz prakse, primjena norme ISO/IEC 27031. Procjene zahtjeva i spremnosti ICT-a za BCM, kritični ICT resursi, procjene ICT rizika sa stajališta BCMS-a. Izrada ICT strategije za BCMS, strukturiranje i arhitektura potrebne ICT opreme za BCMS. (3 sata)

8. Razvoj kompetencija za BCMS i certificiranja za BCMS. Razvoj osobnih kompetencija: Certifikati BCM (ISO22301) Foundation, BCM (ISO22301) Lead Implementer, BCM (ISO22301) Lead Auditor, Risk Manager, Lead Risk Manager, Disaster Recovery Manager). Certifikacija BCMS-a prema normi ISO/IEC 22301. (2 sata)</td></tr>
<tr><td>2.6. Vrste izvođenja nastave:</td><td colspan="2">☒ predavanja
☒ seminari i radionice
☐ vježbe
☐ on line u cijelosti
☒ mješovito e-učenje
☐ terenska nastava</td><td colspan="2">☒ samostalni zadaci
☐ multimedija i mreža
☐ laboratorij
☒ mentorski rad
☐ (ostalo upisati)</td><td colspan="2">2.7. Komentari:</td></tr>
<tr><td>2.8. Obveze studenata</td><td colspan="6">Vježba: identificirati scenarije koji bi mogli dovesti do prekida rada informacijskog sustava ili izvršavanja jednog ili više poslovnih procesa te napraviti analizu njihovog utjecaja na poslovanje na primjeru organizacije</td></tr>
<tr><td rowspan="4">2.9. Praćenje rada studenata (upisati udio u ECTS bodovima za svaku aktivnost tako da ukupni broj ECTS bodova odgovara bodovnoj vrijednosti predmeta):</td><td>Pohađanje nastave</td><td>1</td><td>Istraživanje</td><td></td><td>Praktični rad</td><td>1</td></tr>
<tr><td>Eksperimentalni rad</td><td></td><td>Referat</td><td></td><td>(Ostalo upisati)</td><td></td></tr>
<tr><td>Esej</td><td></td><td>Seminarski rad</td><td></td><td>(Ostalo upisati)</td><td></td></tr>
<tr><td>Kolokviji</td><td></td><td>Usmeni ispit</td><td>1</td><td>(Ostalo upisati)</td><td></td></tr>
</table>

	Pismeni ispit		Projekt	2	(Ostalo upisati)	

2.10. Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	**Naslov**	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**
	ISO 22301:2019, Security and resilience - Business continuity management systems - Requirements (https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en)		DA
	ISO/IEC 27031:2011, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity		DA
	ISO/IEC 27035-1:2016, Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management		DA
	ISO/IEC 27035-2:2016, Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response		DA
	ISO/IEC 27035-3:2020, Information technology - Information security incident management - Part 3: Guidelines for ICT incident response operations		DA

2.11. Dopunska literatura (u trenutku prijave prijedloga studijskoga programa)	• Graham, Julia, and David Kaye. A Risk Management Approach to Business Continuity: Aligning Business Continuity and Corporate Governance. Rothstein Publishing, 2015. • Jim Burtles, K. L. J., and FBCI CMLJ. Principles and Practice of Business Continuity: Tools and Techniques. Rothstein Publishing, 2015. • Hiles, Andrew. Business continuity management: Global best practices. Rothstein Publishing, 2014.

1. OPIS PREDMETA - OPĆE INFORMACIJE			
1.1. Nositelj predmeta	Ivan Magdalenić	1.6. Godina studija	1
1.2. Naziv predmeta	**Upravljanje rizicima informacijske sigurnosti**	1.7. Broj bodova po ECTS sustavu	6 ECTS
1.3. Suradnici	Davor Maček	1.8. Način izvođenja nastave (broj sati P + V + S + e-učenje)	20 + 0 + 10
1.4. Studijski program (preddiplomski, diplomski, integrirani, stručni)	Specijalistički poslijediplomski studij	1.9. Očekivani broj studenata na predmetu	10-15

1.5. Status predmeta	Obavezni	1.10. Razina primjene e-učenja (1., 2., 3. razina), postotak izvođenja predmeta *on line* (maksimalno 20%)	2, 10% izvođenja predmeta on line
2. OPIS PREDMETA			
2.1. Ciljevi predmeta	• Razumijevanje najčešćih sigurnosnih rizika i načina prodora u informacijske sustave kao i oblika zlouporabe informacija/podataka. Iz oblika zlouporabe informacija/podataka određuje se sigurnosni rizik, tip ranjivost te način djelovanja. • Poznavanje i primjena metoda potrebnih za upravljanje mogućim sigurnosnim rizicima, načinima njihovog praćenja te kontrolom i revizijom učinjenih aktivnosti. • Analiza i prepoznavanje potrebnih mjera za kvalitetnim upravljanjem sigurnosnim rizicima i smanjenjem mogućih šteta. Procjena sigurnosnog rizika po različitim kategorijama informacijske imovine, način upravljanja sigurnosnim rizicima te određivanje strategije sigurnosti temeljem toga. • Sinteza i prezentacija programa upravljanja ranjivostima/prijetnjama/rizicima u realnom poslovnom/informacijskom sustavu. • Vrednovanje izvedenih aktivnost tijekom realizacije kolegija.	
2.2. Uvjeti za upis predmeta ili ulazne kompetencije koje su potrebne za predmet	Poznavanje i razumijevanje temeljnih koncepata informacijskog sustava i informacijske sigurnosti. Znanja i vještine usvojeni završetkom diplomskog studija.		
2.3. Ishodi učenja na razini programa kojima predmet pridonosi	1. Primijeniti iskustva dobre prakse prilikom uspostave sustava informacijske sigurnosti u poslovnom/ informacijskom sustavu. 2. Definirati, osmisliti i primijeniti strategiju uspostave sustava informacijske sigurnosti 3. Uspostaviti i unaprjeđivati ciklus planiranja – uspostave – provjere – i – korekcije sustava informacijske sigurnosti. 4. Nadgledati i koordinirati životnim ciklusom informacijske sigurnosti koji uključuje planiranje, nabavu, razvoj, održavanje, vrednovanje i zamjenu sigurnosne infrastrukture. 5. Kritizirati i opravdati odluke iz područja informacijske sigurnosti prema ključnim dionicima (uprava, zaposlenici, klijenti, institucije državne uprave). 6. Primijeniti metodologije procjene i umanjivanja sigurnosnih rizika, te postupke upravljanja rizicima u kontekstu informacijske sigurnosti. 7. Analizirati i procijeniti utjecaj različitih čimbenika (tehničkih, organizacijskih, ljudskih, zakonskih) na sigurnosne rizike.		
2.4. Očekivani ishodi učenja na razini predmeta (3-10 ishoda učenja)	1. Razumjeti značaj podataka i informacija u kontekstu mogućih zlouporaba informacijskog sustava. 2. Razumjeti tehničke, organizacijske i ljudske faktore koji su povezani i koji utječu na rizike u informacijskoj sigurnosti. 3. Procijeniti sigurnosne rizike informacijskog sustava. 4. Poznavati i primijeniti sigurnosne norme i koncepte iz domene upravljanja rizicima u informacijskoj sigurnosti. 5. Poznavati i primijeniti klasifikacijski model ranjivosti te načina postupanja s ranjivostima. 6. Analizirati i primijeniti potrebne mjere za rad sa ranjivostima i prijetnjama. Nastavni plan i program kolegija je sukladan kompetecijama koje definira „Europski okvir e-kompetencija“ (European e-competences Framework) za profile ICT Security Manager i ICT Security Auditor, te u potpunosti pokriva skup znanja i kompetencija iz domene upravljanja rizicima		

- K1 primjena analize rizika, uzimajući u obzir korporativne vrijednosti i interese
- K2 smanjivanje gubitaka u zavisnosti o ulaganjima u razvoj sustava izbjegavanja rizika
- K3 dobre prakse (metodologije) i standardi u analizi rizika

- S1 izraditi plan upravljanja rizicima kako bi se utvrdile potrebne mjere za njihovo smanjivanje
- S2 prezentiranje i objašnjavanje rezultata provedene procjene rizika
- S3 dizajnirati i dokumentirati procese za analizu i upravljanje rizicima
- S4 primijeniti mjere za smanjivanje posljedica i prijetnji

Sadržaj kolegija dijelom odgovara i sljedećim stručnim certifikatima:
- ISACA CRISC Certified in Risk and Information Systems Control
- ISACA CISM Certified Information Security Manager
- (ISC)^2 CISSP Certified Information Systems Security Professional

2.5. Sadržaj predmeta

Nastavna cjelina	**sati**	**ECTS**
Uvod u predmet. Pojam sigurnosnog rizika. Vrste sigurnosnih rizika. Odnos sigurnosni rizik – ranjivost – sigurnosni incident. Procjena sigurnosnog rizika. Načini nastanka sigurnosnih rizika. Pregled mogućih prodora u informacijske sustave i njihove značajke. Traženje sigurnosnih propusta. Analize ranjivosti i moguće posljedice tih ranjivosti. Vjerojatnost njihova nastanka.	5	
Metrike za određivanje sigurnosnih rizika. Kvantitativne i kvalitativne metrike. Metode za procjenu rizika.	4	
Alati za procjenu rizika.	3	
Oblici i posljedice nepostojanja organizacije sigurnosti, definiranje potrebnih odgovornosti i njihovih nositelja, obaveze treće strane u pristupima informacijskim resursima.	4	
Međunarodne norme i koncepti upravljanja sigurnosnim rizicima. Iskustva dobre prakse.	5	**1**
Proces upravljanja sigurnosnim rizicima. Uspostava registra informacijske imovne. Uspostava PDCA ciklusa kao dio procesa upravljanja sigurnosnim rizicima. Rezultat procjene sigurnosnog rizika.	6	
Nepoštivanje međunarodnih propisa iz područja sigurnosti informacija/podataka. Najčešći oblici kršenja nacionalnih propisa i nepoštivanje nacionalnog programa informacijske sigurnosti, te njihov utjecaj na upravljanje sigurnosnim rizicima. Europske direktive iz domene kibernetičke sigurnosti, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga	3	
Ukupno:	**30**	**1**

2.6. Vrste izvođenja nastave	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ on line u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☐ laboratorij ☒ mentorski rad ☐ (ostalo upisati)	Komentari: Nastava na kolegiju se temelji na predavanjima, analizi studija slučajeva iz nabolje prakse, te samostalnom radu studenata u okviru kojeg će studenti izraditi, te prezentirati (i obraniti) proces upravljanja sigurnosnim rizicima u realnom poslovnom/ informacijskom sustavu.
2.7. Obveze studenata	Pohađanje predavanja, izrada i obrada projekta/ seminarskog rada (razrađen i dokumentiran proces upravljanja sigurnosnim rizicima u realnom poslovnom/ informacijskom sustavu), usmeni ispit.		

2.8. Praćenje rada studenata

Pohađanje nastave	DA		Projekt	DA		Pismeni ispit		NE
Eksperimentalni rad			Istraživanje			Usmeni ispit	DA	
Esej			Referat			(ostalo upisati)		NE
Kolokvij			Seminarski rad			(ostalo upisati)		NE
			Praktični rad			Broj bodova po ECTS sustavu (ukupno)	**6**	

2.9. Obvezna literatura (dostupna u knjižnici i/ili na drugi način)

Naslov	**Dostupnost u knjižnici**	**Dostupnost putem ostalih medija**
Tipton, H.F., Krause, M. Information Security Management Handbook (Part 1 – Information Security and Risk Management, Access Control), Sixth Edition, Auerbach publications, CRC Press, 2010.	1	
Vacca, J. R. Computer and Informatio Security Handbook, 3rd Edition, Morgan Kaufmann, 2017.	1	
Peltier, T. R. Information Security Risk Analysis, Second Edition, 2005.	1	
ISO/IEC 27003 — Information security management system implementation guidance	1	DA
ISO/IEC 27004 — Information security management — Measurement	1	DA
ISO/IEC 27005 — Information security risk management	1	DA
ISACA RISK IT Framework, 2nd Edition		DA

2.10. Dopunska literatura (navesti naslov)

- Andress, J. The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress, 2011.
- Hayden, L. IT Security Metrics – A Practical Framework for Measuring Security and Protecting Data, McGraw Hill, 2010.

	• Talabis, M., Martin, J., Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis 1st Edition, Syngrees, 2013. • Wheeler, E., Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngrees, 2017. • Peltier, T. R., Information Security Risk Analysis 3rd Edition, CRC Press, 2010. • Schoenfield, B. S. E., Securing Systems: Applied Security Architecture and Threat Models, CRC Press, 2015. • Kohnke, A., Sigler, K., Shoemaker, D., Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework (Internal Audit and IT Audit), CRC Press, 2018. • Colder, A., Watkins, S. G., Information Security Risk Management for ISO 27001/ISO 27002, IT Governance 2019.

3. Opće informacije za studente

a. prostori i oprema za učenje

SUZG FOI ima 10.800 m² prostora i potrebnu infrastrukturu za izvođenje nastave i istraživačke aktivnosti. SUZG FOI djeluje na tri lokacije: u glavnoj zgradi bivšeg isusovačkog samostana (Pavlinska 2, FOI 1), starog nekoliko stotina godina, u zgradi bivše muzičke škole (Prilaz Fausta Vrančića 3, FOI 2) i u novoobnovljenoj Vili Oršić (Petra Preradovića 15, FOI 3). SUZG FOI je vlasnik zgrada FOI 1 i FOI 2, dok je FOI 3 zgradu SUZG FOI dobio na korištenje od grada Varaždina na 30 godina. Povijesni objekt FOI 1, smješten je na središnjem gradskom trgu u Varaždinu te predstavlja kulturnu baštinu grada Varaždina. Kulturni spomenik je i Vile Oršić (FOI 3), koja je renovirana 2023. godine. SUZG FOI raspolaže s 11 laboratorijskih učionica opremljenih modernim stolnim računalima, a studenti imaju mogućnost donošenja vlastitih uređaja (BYOD). Neke laboratorijske učionice prilagođene su učenju temeljenom na radu i projektima, s posebnim namještajem koji omogućuje lako premještanje i grupiranje studenata. Većina projektora zamijenjena je velikim LCD ekranima kako bi se omogućila visoka grafička kvaliteta i lakše prikazivanje nastavnih materija te hibridna nastava. Studentima su dostupne prostorije za rad od 7 do 21 sat s LCD ekranima i Wi-Fi pristupom, a postoji i mogućnost posudbe računala za akademsku godinu ili kraće (po potrebi). Proces dugotrajne posudbe provodi se putem natječaja, a studenti se prijavljuju, a odluke se donose prema unaprijed definiranim kriterijima, uključujući socio-ekonomski status, akademski uspjeh i izvannastavne aktivnosti. SUZG FOI također koristi iznajmljene prostore u Zagrebu i Sisku za izvođenje stručnog prijediplomskog studija Informacijske tehnologije i digitalizacija poslovanja.

b. podaci vezani uz digitalni identitet, korištenje informacijskom i komunikacijskom tehnologijom

LDAP račun / AAI@EduHr elektronički identitet - LDAP korisničke račune otvaraju administratori CARNetovih ustanova članica,a za ažurnost LDAP imenika cijele @foi.hr domene brinu djelatnici Jedinice za tehničku pomoć izvođenja – CIPa. Mnogi servisi koje studenti koriste tijekom studiranja koriste AAI@EduHR identitet kao autentifikacijski model: e-learning sustav [Moodle], eduroam pristup bežičnoj mreži WLAN unutar zgrade Fakulteta FOI1, FOI2 i FOI3, email sustav, FOI nastava i mnogi drugi. Pregled aplikacija/servisa dostupan je na FOI Apps Launcher.

U nastavi, SUZG FOI koristi Moodle LMS (Learning Management System), digitalno okruženje za učenje koje omogućuje organizaciju, vođenje i praćenje nastavnih aktivnosti. Sustav omogućuje jednostavno kreiranje i distribuciju nastavnih materijala, provođenje online ispita i testova, praćenje napretka studenata te interaktivnu komunikaciju između predavača i studenata putem foruma, chatova i suradničkih alata..

Online platforma BBB za web konferencije i virtualno učenje omogućuje organizaciju i održavanje virtualnih sastanaka, seminara i nastave putem interneta, pružajući korisnicima interaktivno i dinamično okruženje za učenje i suradnju. Sustav je osmišljen kako bi podržao različite oblike online komunikacije, od jednostavnih sastanaka i konzultacija do kompleksnih webinara i virtualnih učionica s velikim brojem sudionika. Sudionici mogu koristiti funkcionalnosti poput dijeljenja zaslona, interaktivne bijele ploče, chata i anketa, dok predavači i organizatori imaju mogućnost nadzora, analize sudjelovanja i snimanja sesija za kasniju upotrebu. Sustav je također prilagođen integraciji s platformama za e-učenje (LMS), što

omogućuje sinkronizaciju nastavnog sadržaja, automatsku evidenciju prisustva i analizu angažmana sudionika.

U proteklih 5 godina SUZG FOI je unaprijedio i modernizirao svoje studijske programe, prateći tehnološke promjene i tržište rada. Uspješno je provedena digitalna transformacija nastavnih i poslovnih procesa. SUZG FOI prednjači u primjeni digitalnih modela učenja i poučavanja, s vlastitom online infrastrukturom koja omogućuje izvođenje online nastave, poslužiteljima, sustavom za e-učenje, sustavom autentifikacije i autorizacije te sustavom za webinare. Kao primjer odgovora na disruptivni potencijal tehnologija SUZG FOI je među prvim institucijama koje su brzo reagirale na izazove primjene novih tehnologija te izradile sveobuhvatan dokument za odgovorno korištenje umjetne inteligencije (UI) u akademskoj zajednici, pokrivajući primjenu u obrazovanju, znanstvenom istraživanju i stručnoj praksi. Dokumentom pod nazivom Okvir korištenja alata umjetne inteligencije u nastavi, studentskim radovima i istraživanju na Sveučilištu u Zagrebu Fakultetu organizacije i informatike, SUZG FOI je istaknuo predanost etičkom, odgovornom i zakonski usklađenom korištenju umjetne inteligencije, u skladu s relevantnim domaćim i međunarodnim zakonima i standardima.

c. informacije o ostvarivanju i zaštiti prava studenata i podrški njima

Student sklapa ugovor o studiranju s Fakultetom. Ugovorom o studiranju pobliže se uređuju međusobna prava i obveze tijekom studija, način financiranja studija, pravila o postupanju s autorskim djelima i pravila o postupanju s pravima industrijskog vlasništva i njihovu iskorištavanju te druga važna pitanja za ugovorne strane.

Student ima pravo na mirovanje obveza: u vrijeme korištenja prava vezanih uz zaštitu roditeljstva (trudnoće, rodiljnog, roditeljskog i posvojiteljskog dopusta), za vrijeme bolovanja dužeg od tri mjeseca, u drugim opravdanim slučajevima predviđenim zakonom, kolektivnim ugovorom ili općim aktom Sveučilišta. Pisani zahtjev za mirovanje prava i obveza s obrazloženjem student podnosi Odboru studija.

Pravilnikom o stegovnoj i materijalnoj odgovornosti studenata i drugih polaznika SUZG FOI-ja „uređuju se pitanja odgovornosti studenata i drugih polaznika Fakulteta vezano uz nepoštivanje zakonskih i drugih propisa i odluka, nadležnosti za pokretanje stegovnog postupka (u daljnjem tekstu postupka), vođenje postupka, način rada i odlučivanja Stegovnog suda, rokovi zastare za pokretanje postupka, provođenje izrečenih mjera, evidenciju izrečenih mjera i drugo u vezi s odgovornošću i provođenjem stegovnog postupka.“

Sukladno članku 3. Pravilnika lakšim stegovnim prijestupom smatrat će se sljedeća djela i postupci:

1. ometanje bilo kojeg oblika nastave, provjere znanja ili drugih službenih aktivnosti Fakulteta;
2. nedopušteno pružanje pomoći drugim studentima na ispitima ili drugim provjerama znanja;
3. nepoštivanje i kršenje unaprijed određenih procedura na Fakultetu;
4. lažno predstavljanje pri provjeri nazočnosti bilo kojeg oblika nastave;
5. ponašanje i odijevanje koje odstupa od opće prihvaćenih pravila za danu priliku;
6. neprimjereno komuniciranje sa zaposlenicima, djelatnicima Fakulteta i drugim studentima/polaznicima;
7. narušavanje čistoće svih prostora Fakulteta;

8. korištenje unutarnjeg i vanjskog prostora Fakulteta za oglašavanje, promidžbu ili prodaju na mjestima koja nisu za to predviđena ili uklanjanje službenih obavijesti sa službenih mjesta za oglašavanje;
9. korištenje unutarnjeg i vanjskog prostora Fakulteta za okupljanja koja nisu dio programa rada Fakulteta i/ili odobrena od strane odgovorne osobe Fakulteta;
10. pribavljanje, umnožavanje ili upotreba ispitnog materijala bez dopuštenja autora tih materijala kao i njihova distribucija;
11. oglušivanje na opomene knjižnice Fakulteta;
12. drugi postupci kojima se narušava ugled Fakulteta

Sukladno članku 3. Pravilnika težim stegovnim prijestupom smatrat će se sljedeća djela i postupci:

1. nasilno ponašanje prema zaposlenicima, djelatnicima i studentima/polaznicima Fakulteta;
2. grubo narušavanje reda (fizičko nasilje, nepristojno i neprimjereno izražavanje ili ponašanje) na nastavi, ispitima, provjerama znanja bilo kojeg oblika u bilo kojim prostorima u posjedu Fakulteta ili na događajima koji su povezani s Fakultetom; poticanje i organiziranje nereda i sudjelovanje u istom;
3. grubo narušavanje ugleda Sveučilišta i Fakulteta i gruba povrede opće prihvaćenih pravila ponašanja, pristojnosti ili dostojanstva učinjene prema zaposlenicima, djelatnicima, studentima/polaznicima Fakulteta, njihovo uznemiravanje i diskriminiranje po bilo kojoj osnovi u prostorima Fakulteta i/ili na događajima koji su povezani s Fakultetom;
4. neovlašteno snimanje ili fotografiranje zaposlenika, djelatnika, studenata/polaznika, opreme i prostorija Fakulteta tijekom nastavnih aktivnosti kao i njihovo distribuiranje;
5. krivotvorenje bilo kojeg dokumenta vezanog uz studij i/ili ostvarenje studentskih prava, neovlašteno unošenje i/ili ispravljanje i krivotvorenje podataka u dokumentima i bazama podataka i sustavima, ka kao i namjerno uništavanje, oštećenje ili onesposobljavanje tih dokumenata;
6. davanje lažnih podataka ili poduzimanje postupaka na temelju kojih student/polaznik ostvaruje neko pravo koje mu ne pripada (unošenja ispravaka u indeks ili drugu službenu ispravu, ISVU sustav protivno službenom propisanom postupku, unošenje ispravaka u ostale (službene) isprave i akte koje je izdao Fakultet ili Sveučilište, korištenje lažnih dokumenata ili iskaza radi ostvarivanja nekih prava koja mu ne pripadaju);
7. lažno predstavljanje i/ili prijavljivanje na provjerama znanja svih oblika, polaganje ispita ili drugih oblika provjere znanja umjesto drugog studenta ili polaznika, kao i omogućavanje ovih postupaka;
8. plagiranje u pisanom obliku djela nekog autora (drugog studenta, nastavnika, treće osobe ili izvora na Internetu, uključujući samog sebe) bez navođenja izvora;
9. korištenje umjetne inteligencije na način kako nije dozvoljeno Okvirom korištenja alata umjetne inteligencije u nastavi, studentskim radovima i istraživanju na Fakultetu i/ili drugim aktima Fakulteta;
10. prepisivanje ili uporaba nedozvoljenih pomagala za prepisivanje na ispitima, odnosno na provjerama znanja bilo kojeg oblika (primanje pomoći u rješavanju zadataka postavljenim na ispitima ili drugim provjerama znanja; komunikacija s osobama izvan prostorije u kojoj se provodi

provjera znanja; uporaba nedozvoljenih nastavnih materijala na ispitima i/ili provjerama znanja računala, pametnih telefona i slično, osim u slučajevima kad su eksplicitno dopušteni);

11. narušavanje sigurnosti i integriteta informacijskog sustava Fakulteta i Sveučilišta u Zagrebu (u daljnjem tekstu: Sveučilište), narušavanje sigurnosti i integriteta podataka koji su pohranjeni ili se prenose tim informacijskim sustavom, narušavanje prava na privatnost drugih korisnika informacijskog sustava kao i zloporaba tuđih resursa u sklopu informacijskog sustava;
12. korištenje informacijskih resursa Fakulteta i Sveučilišta za ugrožavanje drugih informacijskih sustava i privatnosti drugih osoba kao i nepridržavanje propisanih mjera i sredstava zaštite sigurnosti informacijskog sustava Fakulteta;
13. otuđivanje odnosno neovlašteno kopiranje računalnih programa koji se koriste na Fakultetu te korištenje ili distribuiranje drugih resursa zaštićenih pravima autorskog i intelektualnog vlasništva;
14. namjerno uništavanje, otuđivanje ili oštećivanje imovine Fakulteta, djelatnika Fakulteta ili drugih studenata i polaznika Fakulteta;
15. posredno i neposredno nuđenje novca, materijalne vrijednosti ili druge imovinske koristi te bilo kakav postupak utjecanja ili pritisaka na nastavnike ili ostale zaposlenike Fakulteta;
16. javno zastupanje ili predstavljanje Fakulteta, bilo koje sastavnice, studentske organizacije ili drugog člana/članice sveučilište zajednice bez dopuštenja ovlaštenih osoba;
17. javno iznošenje neprovjerenih i netočnih podataka o drugim studentima/studenticama i ostalim članovima sveučilišne zajednice;
18. dolazak na bilo koji od oblika nastave pod utjecajem alkohola ili opojnih droga narkotika te lijekova osim ako isti nisu medicinski indicirani;
19. svi postupci i radnje koji su Zakonom predviđeni kao kaznena djela;
20. ponavljanje lakših stegovnih prijestupa više od dva puta tijekom studija.

Za lakša stegovna djela može se izreći pisana opomena. Za teža stegovna djela može se izreći jedna od sljedećih mjera:

1. pisana javna opomena za slučajeve kada je student/polaznik prvi puta prijavljen i kada se smatra da se njome može postići svrha kažnjavanja posljednja opomena pred isključenje
2. zabrana polaganja ispita i/ili pohađanja određenih oblika nastave do godinu dana ili do isteka akademske godine; (može uključivati i kolokviranje i predaju/obranu projekta i slično)
3. izuzimanje od međunarodne razmjene od 6 mjeseci do 2 godine
4. zabrana upisa više godine studija
5. isključenje s Fakulteta do dvije godine koje obuhvaća zabranu pristupa ISVU
6. sustavu, upis semestra, ovjera godine studija, polaganje ispita i sudjelovanje u drugim oblicima nastave
7. trajno isključenje s Fakulteta koje podrazumijeva prestanak statusa studenta i svih prava koja iz toga proizlaze. Student više nema pravo upisati bilo koji studij/program na Fakultetu.

Pravo na pristup informacijama koje posjeduje SUZG FOI uređeno je Zakonom o pravu na pristup informacijama (NN 25/13, 85/15, 69/22). Zakon daje svim domaćim i stranim fizičkim i pravnim osobama, na jednak način i pod jednakim uvjetima pravo na pristup informacijama. Zakonom se propisuju načela

prava na pristup informacijama i ponovnu uporabu informacija, ograničenja prava na pristup informacijama i ponovnu uporabu informacija, postupak za ostvarivanje i zaštitu prava na pristup informacijama i ponovnu uporabu informacija. SZFOI provodi zaštitu osobnih podataka u skladu s Općom uredbom o zaštiti podataka i Zakonom o provedbi Opće uredbe o zaštiti podataka. Više podataka moguće je pronaći na mrežnim stranicama Fakulteta - Zaštita osobnih podataka.

Visoko učilište sustavno rješava probleme plagiranja, prepisivanja i krivotvorenja rezultata. Nastavnici i mentori su dužni svaki slučaj plagiranja, prepisivanja i/ili krivotvorenja rezultata prijaviti, a povjerenstvo sankcionirati u skladu s Pravilnikom o stegovnoj i materijalnoj odgovornosti studenata i drugih polaznika.

d. informacije o podršci studentima

SUZG FOI već tijekom upisa te za cijelo vrijeme studiranja svojim studentima osigurava dostatne i lako dostupne resurse kako bi im olakšao tijek studija. Studentima su dostupne različite službe, uredi i centri koji su definirani ustrojem Fakulteta.

Odjel za studentske poslove sastoji se od Referade za prijediplomski i diplomski studij te Referade za poslijediplomske studije. Referada je centralno mjesto na kojem studenti mogu dobiti potrebne informacije i savjete o svojem studiju koje su sadržane u pravilnicima o studijima objavljenima zajedno s ostalim relevantnim odlukama na web stranici za svaki studij. Referada je studentima dostupna tijekom cijelog radnog vremena od ponedjeljka do petka putem e-pošte i telefona, a studenti se primaju svaki radni dan od 9.00 do 13.00 sati.

Jedinica za tehničku pomoć izvođenja nastave / Centar za informatičku podršku (CIP) studentima osigurava sve informacije, pomoć i savjete oko elektroničkog identiteta, korisničkih računa, rada s e-mail servisom i akademskih licenci. Pružaju podršku za računala i alate koje koriste nastavnici i studenti na vježbama na računalima te rješavaju razne tehničke poteškoće. Upute i savjeti također su objavljeni na posebnoj web stranici jedinice, a studenti im se, osim osobno, mogu za pomoć obratiti i mailom ili telefonom (npr. upute za promjenu LDAP lozinke).

Knjižnica SUZG FOI upisana je u Upisnik knjižnica u Republici Hrvatskoj (Broj upisnog lista: K-1443/6). Smještena je na lokaciji FOI-1 (Varaždin, Pavlinska ulica 2), u podrumskim prostorijama južnog krila zgrade. Radno vrijeme knjižnice je od ponedjeljka do petka od 7:00 do 20:00 sati (ukupno 65 sati tjedno). Prostor knjižnice sastoji se od ulaznog dijela s informacijskim pultom, čitaonice za tihi rad s 12 radnih mjesta te računalne radionice s 11 radnih mjesta te dodatna dva računala za pretraživanje kataloga i ostalih informacija knjižnice. Prostor namijenjen korisnicima je 150 m², dok je ukupni prostor knjižnice je 200 m² Knjižnica je opremljena suvremenom IT opremom, a prostor knjižnice pokriven je bežičnom mrežom sa slobodnim pristupom. Čitaonica je opremljena i s priključnim mjestima za osobna prijenosna računala korisnika.

Fond knjižnice SUZG FOI sastoji se od 11 841 naslova, odnosno 16 426 svezaka monografskih publikacija, te 284 naslova, odnosno 2523 svezaka ili 10 586 sveščića periodike. Od ukupnog broja monografskih publikacija 4 284 je naslova, odnosno 7 995 primjeraka udžbenika. Ukupan broj naslova udžbenika obvezne literature je 822, a broj primjeraka je 3 101. Knjižnični fond razvrstan je u 19 zbirki. Nabava knjižničnog fonda temelji se na potrebama nastavnih planova i programa, potrebama znanstveno-istraživačkog rada, projekata te potrebama studenata i djelatnika. Nabavlja se relevantna i recentna literatura što se može pratiti po godištima izdanja. Osnovna literatura nabavlja se u pet primjeraka, a dodatna literatura u tri primjerka ili po preporuci predmetnog nastavnika, pri čemu je jedan primjerak

osnovne ili dodatne literature uvijek dostupan korisnicima u čitaonici, u Zbirci osnovne i dodatne literature. Također, korištenjem informacijsko-komunikacijskih tehnologija kojima su opremljeni prostori čitaonica, nastavni laboratoriji i uredi nastavnika omogućen je pristup literaturi pohranjenoj u elektroničkom obliku u repozitorijima s otvorenim pristupom.

Knjižnica SUZG FOI svojim korisnicima (djelatnicima i studentima) osigurava pristup relevantnim izvorima informacija. Mrežna stranica SUZG FOI knjižnice pruža korisnicima osnovne informacije o knjižnici, fondu knjižnice, mrežnim izvorima literature, uslugama knjižnice, upućuje na različite pomoći korisnicima, kao na primjer Upute korisnicima knjižnice, omogućuje pristup virtualnim izložbama, te informira korisnike o kulturnim događanjima u Varaždinu. Središnji dio mrežne stranice informira korisnike o novostima vezanim za knjižnicu, knjižničnu građu i knjižnična događanja. Sve mrežne sadržaje izrađuje i ažurira knjižnica. Knjižnica SUZG FOI koristi knjižnični programski paket MetelWin. Mrežni katalog knjižnice mjesto je koje okuplja svu knjižnu i neknjižnu, tiskanu, digitalnu i digitaliziranu građu te građu na mreži, a koja je inventarizirana i katalogizirana. Katalogizirana mrežna građa je u slobodnom pristupu ili joj se pristupa pomoću AAI@EduHr identiteta. Mrežni katalog knjižnice uključen je u skupni katalog Metel i Hrvatski nacionalni skupni katalog. Katalog knjižnice dostupan je korisnicima putem sustava za e-učenje Moodle, a sustav Moodle dostupan je putem kataloga knjižnice (u desnom izborniku). Ova unakrsna povezanost omogućuje korisnicima pristup željenim sadržajima s jednog mjesta. Svaki korisnik knjižnice ima svoj korisnički račun kojem pristupa AAI@EduHr identitetom. Korisnički račun omogućuje praćenje trenutnog zaduženja, arhivu posudbe, rezervaciju građe, produženje zaduženja te stvaranje liste želja.

Knjižnica SUZG FOI održava web stranicu s mrežnim izvorima i repozitorijima u kojima su pohranjeni radovi djelatnika i studenata u otvorenom pristupu. Mrežna stranica Mrežni izvori literature na jednom mjestu okupljaju dostupne mrežne izvore namijenjene djelatnicima i studentima:

- Summon - sučelje za objedinjeno pretraživanje svih dostupnih pretplaćenih e-izvora u nacionalnoj licenci, e-izvora u otvorenom pristupu i skupnog digitalnog repozitorija Dabar,
- Portal elektroničkih izvora pretplaćenih za hrvatsku akademsku i znanstvenu zajednicu,
- Privremeni pristupi bazama podataka,
- Otvoreni pristup bazama i repozitorijima,
- Digitalna knjižnica EFZG, zbirka digitalnih publikacija s područja ekonomije čiji su nakladnici visokoškolske ustanove iz zemlje i inozemstva. Zbirka je namijenjena svim korisnicima knjižnice FOI pomoću pristupnih podataka koji se mogu dobiti u knjižnici,
- Portal CroRIS – Informacijskom sustavu znanosti RH,
- Digitalni akademski arhiv i repozitorij Dabar FOI,
- Skupni Digitalni akademski arhiv i repozitorij DABAR,
- Portal znanstvenih časopisa RH, HRČAK.

Knjižnica u Digitalnom katalogu pohranjuje i omogućava otvoreni pristup ocjenskim radovima studenata (Zbirka doktorskih radova, Zbirka završnih specijalističkih radova).
Ured za studente s invaliditetom na SUZG FOI osigurava potporu studentima s invaliditetom u okviru centralnog Ureda za studente s invaliditetom UNIZG, prvenstveno vezano uz osiguravanje prava na prilagodbu nastavnog procesa i polaganja ispita. Ured svakom studentu s invaliditetom osigurava individualni pristup u rješavanju izazova prilikom studiranja, a također potiče studente da se uključe u kolegij SUZG Vršnjačka potpora studentima s invaliditetom.

Ured za međunarodnu suradnju daje potporu studentima za mobilnost u sklopu Erasmus+ studijskog boravka i Erasmus+ stručne prakse, ali i za kraće mobilnosti, kao što je Erasmus+ Blended Intensive

Programme (BIP), CEEPUS i DAAD mobilnosti. Isto tako, Ured daje podršku studentima na dolaznoj mobilnosti, uključujući pomoć pri pribavljanju potrebne dokumentacije, prilagodbu i rješavanje problema tijekom boravka na SUZG FOI.

Centar za volontiranje i humanitarni rad djeluje na SUZG FOI 12 godina s ciljem uključivanja studenata u razne aktivnosti koje omogućuju neformalno učenje, odnosno stjecanje dodatnih kompetencija kroz volontiranje, a također povezuje studente i s drugim organizatorima volontiranja.

Studentski zbor je tijelo za pomoć studentima i brigu za ostvarivanje njihovih prava, ali i pokretanje raznih studentskih projekata, kao i humanitarnih i volonterskih akcija. U sklopu Studentskog zbora djeluje i studentski pravobranitelj, dok studentskog savjetnika bira Uprava SUZG FOI iz redova svih studenata koji se prijave na natječaj.

Centar za razvoj programskih proizvoda također daje podršku studentima, odnosno gore navedenim aktivnostima, jer razvija aplikacije koje znatno olakšavaju studiranje (FOI Forms, FOI Radovi, stručna praksa).

Nastavnici i suradnici na SUZG FOI svaki tjedan održavaju konzultacije koje trebaju biti raspoređene u dva radna dana, a svi termini također su objavljeni u aplikaciji FOI Nastava.

Odbor, na prijedlog studenta, predlaže studentu mentora iz redova nastavnika Fakulteta izabranih na znanstveno-nastavna radna mjesta. Studentu se iznimno za mentora može predložiti osoba zaposlena na znanstvenom ili znanstveno-nastavnom radnom mjestu koja nije zaposlenik Fakulteta ili istaknuti stručnjak s akademskim stupnjem doktora znanosti koji nije zaposlenik Fakulteta, pri čemu se u tim slučajevima predlaže i sumentor, zaposlenik Fakulteta. Odluku o imenovanju mentora donosi Fakultetsko vijeće.

Sve informacije su studentima dostupne u e-kolegiju specijalističkog studija Upravljanje sigurnošću i revizija informacijskih sustava. U navedenom e-kolegiju dostupne su informacije i popratni dokumenti o specijalističkom studiju na SZFOI-ja, Materijali za projekt/esej/seminarski ili završni rad i Raspored nastave.