

Predmet:	Osnove informacijske sigurnosti																																					
Nositelji:	Prof. dr. sc. Nikola Hadjina																																					
Opis:	<p>Sve veća važnost i prisutnost informacijskih sustava u poslovanju i ostvarenju poslovnih ciljeva postavlja informacijsku sigurnost u centar suvremenih sustava. Predmet daje temeljna znanja u informacijskoj sigurnosti iz tehničke, administrativne i upravljačke perspektive. Glavne teme predmeta uključuju osnovu kriptografije, kontrole pristupa, opće ranjivosti softvera, opće ranjivosti računalnih mreža, upravljanje digitalnim pravima, klasifikaciju podataka, politike informacijske sigurnosti i zakonske propise, privatnost, utjecaj ljudskog faktora i upravljanje informacijskom sigurnošću te specijalistička poglavlja u informacijskoj sigurnosti. Također se obrađuju teme učinkovitog upravljanja svim aspektima organizacijskih rješenja za računalnu i mrežnu sigurnost te utjecaj sigurnosne tehnologije na upravljanje rizicima informacijske sigurnosti.</p> <p>Posebna pažnja bit će posvećena uspostavi sustava upravljanja informacijskom sigurnošću (ISMS) primjenom međunarodne norme ISO/IEC 27001 te odabiru sigurnosnih mjera prema normi ISO/IEC 27002 kao i svim aktivnostima vezanim na PDCA (Plan-Do-Check-Act) životni ciklus ISMS sustava. U kontekstu uspostave ISMS-a obraditi će se i tema upravljanja kontinuitetom poslovanja (BCM) i analiza utjecaja na poslovanje (BIA).</p> <p>Dodatni materijali pokrivaju zakonske aspekte, revizije informacijske sigurnosti te kako ostvariti sustav upravljanja u organizaciji na dnevnoj razini operativnosti.</p> <p>Osim toga u kolegij su uključene i osnove računalne sigurnosti: sigurnost operacijskih sustava, mrežna sigurnost, vatrozidovi, obrana i DoS napadi, tehnike autentifikacije, sigurnost Weba, tehnike detekcije i sprječavanja upada, sigurnosne tehnike zaštite mobilnog koda, tehnike zaštite privatnosti na Internetu i ostali aspekti računalne sigurnosti. Preduvjeti za ovaj predmet uključuju osnovna znanja o računalnim sustavima i mrežama, poznavanje programiranja i osnovna matematička znanja, ali se ne zahtijeva bilo kakvo prethodno poznavanje računalne i komunikacijske sigurnosti.</p>																																					
ECTS:	6																																					
Sati nastave:	30																																					
Kompetencije:	Studenti će steći osnove razumijevanja postupaka za uključivanje informacijske sigurnosti u informacijske sustave kroz perspektivu sigurnosnog inženjerstva i poslovnog upravljanja. Pored toga steći će praktična iskustava u uspostavi sustava upravljanja informacijskom sigurnošću prema međunarodnim normama i zakonskim propisima.																																					
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi																																					
Nastavne cjeline:	<table border="1"> <thead> <tr> <th>Naziv</th> <th>Sati</th> </tr> </thead> <tbody> <tr> <td>Definiranje informacijske sigurnosti, problemi, ciljevi, načela i politika sigurnosti. Informacijska imovina.</td> <td>1</td> </tr> <tr> <td>Ranjivosti informacijske imovine te prijetnje i napadi na nju.</td> <td>1</td> </tr> <tr> <td>Analiza, upravljanje i nadzor rizika. Metode procjene rizika.</td> <td>2</td> </tr> <tr> <td>Osnove kriptografije. Protokoli, tehnike i algoritmi. Digitalno potpisivanje.</td> <td>2</td> </tr> <tr> <td>Arhitektura sigurnosnog sustava-osnovni moduli (SABSA model). Strategija informacijske sigurnosti.</td> <td>2</td> </tr> <tr> <td>Postupci digitalne identifikacije i autentifikacije.</td> <td>2</td> </tr> <tr> <td>Kontrola pristupa. Matematički modeli. Sigurnosne politike. Dodjela i upravljanje pravima pristupa.</td> <td>2</td> </tr> <tr> <td>Sigurnost i zaštita programa i operacijskih sustava. Povjerljivi sustavi.</td> <td>2</td> </tr> <tr> <td>Sigurnost baza podataka. Transakcijska obrada u višerazinskim sigurnosnim bazama podataka.</td> <td>2</td> </tr> <tr> <td>Sigurnost računalnih mreža i distribuiranih sustava. Višerazinske računalne mreže.</td> <td>1</td> </tr> <tr> <td>Sustavi za detekciju sigurnosnih proboja (IDS/IPS).</td> <td>1</td> </tr> <tr> <td>Projektiranje i izgradnja sustava informacijske sigurnosti (ISMS) prema međunarodnim normama ISO 27001 i ISO 27002.</td> <td>2</td> </tr> <tr> <td>Sigurnosne kontrole - odabir i implementacija prema standardu ISO 27002.</td> <td>2</td> </tr> <tr> <td>Upravljanje, poboljšanje i nadzor sustava informacijske sigurnosti (ISMS) - PDCA ciklus. Mjerenje učinkovitosti kontrola.</td> <td>2</td> </tr> <tr> <td>Upravljanje kontinuitetom poslovanja (BCM). Analiza utjecaja na poslovanje - BIA (Business Impact Analysis).</td> <td>2</td> </tr> <tr> <td>Standardi i kriteriji vrednovanja informacijske sigurnosti.</td> <td>2</td> </tr> <tr> <td>Zakonski i etički aspekti informacijske sigurnosti.</td> <td>2</td> </tr> </tbody> </table>	Naziv	Sati	Definiranje informacijske sigurnosti, problemi, ciljevi, načela i politika sigurnosti. Informacijska imovina.	1	Ranjivosti informacijske imovine te prijetnje i napadi na nju.	1	Analiza, upravljanje i nadzor rizika. Metode procjene rizika.	2	Osnove kriptografije. Protokoli, tehnike i algoritmi. Digitalno potpisivanje.	2	Arhitektura sigurnosnog sustava-osnovni moduli (SABSA model). Strategija informacijske sigurnosti.	2	Postupci digitalne identifikacije i autentifikacije.	2	Kontrola pristupa. Matematički modeli. Sigurnosne politike. Dodjela i upravljanje pravima pristupa.	2	Sigurnost i zaštita programa i operacijskih sustava. Povjerljivi sustavi.	2	Sigurnost baza podataka. Transakcijska obrada u višerazinskim sigurnosnim bazama podataka.	2	Sigurnost računalnih mreža i distribuiranih sustava. Višerazinske računalne mreže.	1	Sustavi za detekciju sigurnosnih proboja (IDS/IPS).	1	Projektiranje i izgradnja sustava informacijske sigurnosti (ISMS) prema međunarodnim normama ISO 27001 i ISO 27002.	2	Sigurnosne kontrole - odabir i implementacija prema standardu ISO 27002.	2	Upravljanje, poboljšanje i nadzor sustava informacijske sigurnosti (ISMS) - PDCA ciklus. Mjerenje učinkovitosti kontrola.	2	Upravljanje kontinuitetom poslovanja (BCM). Analiza utjecaja na poslovanje - BIA (Business Impact Analysis).	2	Standardi i kriteriji vrednovanja informacijske sigurnosti.	2	Zakonski i etički aspekti informacijske sigurnosti.	2	
Naziv	Sati																																					
Definiranje informacijske sigurnosti, problemi, ciljevi, načela i politika sigurnosti. Informacijska imovina.	1																																					
Ranjivosti informacijske imovine te prijetnje i napadi na nju.	1																																					
Analiza, upravljanje i nadzor rizika. Metode procjene rizika.	2																																					
Osnove kriptografije. Protokoli, tehnike i algoritmi. Digitalno potpisivanje.	2																																					
Arhitektura sigurnosnog sustava-osnovni moduli (SABSA model). Strategija informacijske sigurnosti.	2																																					
Postupci digitalne identifikacije i autentifikacije.	2																																					
Kontrola pristupa. Matematički modeli. Sigurnosne politike. Dodjela i upravljanje pravima pristupa.	2																																					
Sigurnost i zaštita programa i operacijskih sustava. Povjerljivi sustavi.	2																																					
Sigurnost baza podataka. Transakcijska obrada u višerazinskim sigurnosnim bazama podataka.	2																																					
Sigurnost računalnih mreža i distribuiranih sustava. Višerazinske računalne mreže.	1																																					
Sustavi za detekciju sigurnosnih proboja (IDS/IPS).	1																																					
Projektiranje i izgradnja sustava informacijske sigurnosti (ISMS) prema međunarodnim normama ISO 27001 i ISO 27002.	2																																					
Sigurnosne kontrole - odabir i implementacija prema standardu ISO 27002.	2																																					
Upravljanje, poboljšanje i nadzor sustava informacijske sigurnosti (ISMS) - PDCA ciklus. Mjerenje učinkovitosti kontrola.	2																																					
Upravljanje kontinuitetom poslovanja (BCM). Analiza utjecaja na poslovanje - BIA (Business Impact Analysis).	2																																					
Standardi i kriteriji vrednovanja informacijske sigurnosti.	2																																					
Zakonski i etički aspekti informacijske sigurnosti.	2																																					
Način polaganja:	Seminarski rad, usmeni ispit																																					
Literatura:	Donald L. Pipkin, „Information Security“, Prentice Hall PTR, 2000 Dieter Gollman, „Computer Security“, John Wiley & Sons, 1999 Andrew Blyth, Gerald L. Kovacich, „Information Assurance“, Springer- Verlag London Limited, 2001 Harold F. Tipton, Micki Krause, "Information Security Management", Handbook, 4 th edition, CRC Press LLC, 2000																																					
Semestar:	1																																					
Izvođenje na engleskom:	Da																																					
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.																																					

Predmet:	Sigurnost računalnih mreža	
Nositelji:	Prof. dr. sc. Miljenko Mikuc, Prof. dr. sc. Gordan Gledec, doc.dr.sc. Stjepan Groš	
Opis:	<p>Informacijski sustavi su osnova modernog poslovanja. Temeljna infrastruktura na kojoj se baziraju su, između ostalog, i računalne mreže te Internet kao najpoznatija mreža. Zbog toga je izuzetno važno da se studenti upoznaju sa sigurnosnim problemima današnjih računalnih mreža i načinima na koji se ti problemi rješavaju, odnosno ublažuju. U sklopu predmeta proći će se po različitim slojevima računalne mreže te će se u svakom sloju ukazati na probleme i njihova rješenja. Poseban naglasak bit će na TCP/IP porodici protokola.</p> <p>Preduvjeti za ovaj predmet uključuju osnovna znanja o računalnim mrežama i operacijskim sustavima, poznavanje programiranja i osnovna matematička znanja, uključivši osnovna znanja o kriptografskim algoritmima.</p>	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	<p>Studenti će steći osnovna razumijevanja sigurnosnih problema u današnjim računalnim mrežama koja će im omogućiti planiranje i provođenje zaštite računalnih mreža. Pored toga steći će praktična iskustava koja će im omogućiti korištenje osnovnih zaštitnih mehanizama te će također steći osnovne vještine potrebne za provjeru sigurnosti postojećih računalnih mreža.</p>	
Oblici provođenja nastave:	Predavanja i seminarski radovi	
Nastavne cjeline:	Naziv	Sati
	Temeljni mrežne i računalne sigurnosti	2
	Sigurnost podatkovnog sloja i Ethernet lokalnih mreža	2
	Sigurnost bežičnih mreža	4
	Sigurnost mrežnog sloja Interneta	2
	Sigurnost prijenosnog sloja Interneta	2
	Sustavi autentifikacije i autorizacije	2
	Sigurnost najkorištenijih internetskih usluga	4
	Sigurnost web-aplikacija	4
	Taksonomija ranjivosti i prijetnji	1
Metode provaljivanja i penetracijski testovi	5	
Način polaganja:	Seminarski rad.	
Literatura:	<p>Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, 5th edition, McGraw Hill Professional, 2005.</p> <p>Chris Hurley, Penetration Tester's Open Source Toolkit, Volume 2, Syngress, 2007.</p> <p>Različiti materijali i podaci dostupni na Internetu</p>	
Semestar:	1	
Izvođenje na engleskom:	Da	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Upravljanje sigurnosnim rizicima																											
Nositelji:	Prof. dr. sc. Nikola Hadjina																											
Opis:	<p>Predmet razmatra pitanja informacijske sigurnosti kao upravljačkog procesa kojemu je cilj osigurati poslovne procese i njihov kontinuitet te informacijsku imovinu poslovnog subjekta. Nekoliko je tema koje se u sklopu kolegija analiziraju: pitanje potrebnih investicija u sigurnost, način postizanja željene razine sigurnosti te konkretna ugradnja sigurnosne strategije. Sadržaj se odnosi na usporednu analizu komercijalno raspoloživih alata za upravljanje rizikom, te kriterija koji se tiču izbora metodološke podrške problemu procjene rizika. Dodatno se pojašnjava i način njihove primjene u kontekstu gospodarstva i javnog sektora. Pri analiziranju pitanja potrebnih ulaganja u sigurnost razmatraju se svi čimbenici koji utječu na veličinu investicija kao što je veličina rizika, potrebe za unapređenjem sigurnosti koje proizlaze iz propisa i zahtjeva poslovnih partnera, potreba diferencijacije na tržištu i drugo. Kao instrument utvrđivanja potrebnih investicija u sigurnost posebno se pojašnjava analiza i procjena rizika te veličine za procjenu rizika. Naglasak je na nematerijalnoj informacijskoj imovini, njenoj važnosti i ulozi u poslovnom procesu te načinu njene zaštite. Kao dio problema utvrđivanja rizika pojašnjava se i rizik eksternalizacije i njegov utjecaj na poslovanje. Kao način postizanja sigurnosti studentima će biti razjašnjene aktualne norme i koncepti sigurnosti te njihova primjena. Posebna se pažnja posvećuje organizacijskoj razini sigurnosti odnosno sigurnosnim politikama te njihovoj strukturi i formi. Studenti će biti upućeni na probleme oblikovanja, donošenja i ugradnje sigurnosnih politika u kontekstu specifičnih zahtjeva sredine u kojoj se primjenjuju. Studenti će biti upoznati i sa zakonima iz područja informacijske sigurnosti kao jednim od izvora zahtjeva na informacijsku sigurnost. Preduvjet su znanja stečena na diplomskom studiju.</p>																											
ECTS:	6																											
Sati nastave:	30																											
Kompetencije:	<p>Studenti će naučiti kako primjenom različitih tehnika i analitičkih alata utvrditi veličinu informacijskih rizika te odrediti strategiju sigurnosti. Po završetku ovog kolegija studenti će dobiti znanja o:</p> <ul style="list-style-type: none"> • načinu pristupa procjeni rizika za različite kategorije informacijske imovine, • načinu uspostave procesa upravljanja informacijskim rizikom, • utvrđivanju i praktičnom provođenju procesa upravljanja rizikom, • aktualnim normama i konceptima upravljanja rizikom. <p>Na kraju kolegija od studenata se očekuje da su upoznati s ključnim problemima iz područja upravljanja rizicima i informacijskom sigurnošću te da poznaju način provedbe politika sigurnosti u poslovnoj sredini.</p>																											
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.																											
Nastavne cjeline:	<table border="1"> <thead> <tr> <th>Naziv</th> <th>Sati</th> </tr> </thead> <tbody> <tr> <td>Pojam sigurnosnog rizika i razlozi nastanka</td> <td>2</td> </tr> <tr> <td>Analiza i procjena rizika. Materijalna i nematerijalna imovina. Prijetnje sigurnosti i vjerojatnost njihova nastanka. Ranjivost IS-a.</td> <td>2</td> </tr> <tr> <td>Metrika rizika. Kvalitativna i kvantitativna metrika.</td> <td>2</td> </tr> <tr> <td>Metode za procjenu rizika. Cjelovite metode. Pomoćne metode i tehnike.</td> <td>2</td> </tr> <tr> <td>Programska podrška procjeni rizika.</td> <td>3</td> </tr> <tr> <td>Upravljanje rizikom kao instrument unapređivanja sigurnosti. ISO/BS norme.</td> <td>2</td> </tr> <tr> <td>Ostali koncepti unapređenja sigurnosti. Zakoni i zahtjevi struke.</td> <td>2</td> </tr> <tr> <td>Rezultati upravljanja rizikom. Registar imovine. Izvješće o procijenjenom riziku.</td> <td>3</td> </tr> <tr> <td>Analiza utjecaja na poslovanje. Plan obrade rizika.</td> <td>3</td> </tr> <tr> <td>Uspostava procesa upravljanja rizikom. PDCA ciklus</td> <td>3</td> </tr> <tr> <td>Planiranje ISMS-a i priprema dokumentacije. Implementacija sigurnosnih kontrola.</td> <td>3</td> </tr> <tr> <td>Primjeri iz prakse.</td> <td>3</td> </tr> </tbody> </table>	Naziv	Sati	Pojam sigurnosnog rizika i razlozi nastanka	2	Analiza i procjena rizika. Materijalna i nematerijalna imovina. Prijetnje sigurnosti i vjerojatnost njihova nastanka. Ranjivost IS-a.	2	Metrika rizika. Kvalitativna i kvantitativna metrika.	2	Metode za procjenu rizika. Cjelovite metode. Pomoćne metode i tehnike.	2	Programska podrška procjeni rizika.	3	Upravljanje rizikom kao instrument unapređivanja sigurnosti. ISO/BS norme.	2	Ostali koncepti unapređenja sigurnosti. Zakoni i zahtjevi struke.	2	Rezultati upravljanja rizikom. Registar imovine. Izvješće o procijenjenom riziku.	3	Analiza utjecaja na poslovanje. Plan obrade rizika.	3	Uspostava procesa upravljanja rizikom. PDCA ciklus	3	Planiranje ISMS-a i priprema dokumentacije. Implementacija sigurnosnih kontrola.	3	Primjeri iz prakse.	3	
Naziv	Sati																											
Pojam sigurnosnog rizika i razlozi nastanka	2																											
Analiza i procjena rizika. Materijalna i nematerijalna imovina. Prijetnje sigurnosti i vjerojatnost njihova nastanka. Ranjivost IS-a.	2																											
Metrika rizika. Kvalitativna i kvantitativna metrika.	2																											
Metode za procjenu rizika. Cjelovite metode. Pomoćne metode i tehnike.	2																											
Programska podrška procjeni rizika.	3																											
Upravljanje rizikom kao instrument unapređivanja sigurnosti. ISO/BS norme.	2																											
Ostali koncepti unapređenja sigurnosti. Zakoni i zahtjevi struke.	2																											
Rezultati upravljanja rizikom. Registar imovine. Izvješće o procijenjenom riziku.	3																											
Analiza utjecaja na poslovanje. Plan obrade rizika.	3																											
Uspostava procesa upravljanja rizikom. PDCA ciklus	3																											
Planiranje ISMS-a i priprema dokumentacije. Implementacija sigurnosnih kontrola.	3																											
Primjeri iz prakse.	3																											
Način polaganja:	Seminarski rad, usmeni ispit																											
Literatura:	<p>Information Security Policies and Procedures: A Practitioner's Reference, Second Edition, Thomas R. Peltier, 2004. BS 7799-3:2006 - Risk Management Guidelines (Hardcopy) Information Security Risk Analysis, Second Edition, Thomas R. Peltier, 2005.</p>																											
Semestar:	2																											
Izvođenje na engleskom:	Da																											
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.																											

Predmet:	Biometrijski postupci autentifikacije	
Nositelji:	Prof. dr. sc. Slobodan Ribarić, Prof. dr. sc. Sven Lončarić	
Opis:	Postupci autentifikacije identiteta u informacijskim sustavima i informacijskom društvu. Temelji obrade i analize biometrijskih signala i slika. Temelji raspoznavanja uzoraka. Temelji teorije detekcije. Pregled metoda i tehnologija za biometrijsku autentifikaciju. Autentifikacijski protokoli temeljeni na otisku prsta, slici lica, šarenici, mrežnici, otisku dlana, geometriji ruke i dlana, potpisu, govoru i DNK. Postupci registracije korisnika u bazi, verifikacija i identifikacija. Vrednovanje kvalitete i učinkovitosti biometrijskih mehanizama (FRR, FAR, FER, EER). Primjena biometrijskih postupaka u kontroli pristupa i autorizaciji korištenja informacijskih sustava. Korištenje pametnih kartica s biometrijskim karakteristikama. Upravljanje u biometriji, što uključuje prikupljanje, distribuciju i obradu biometrijskih podataka, u cilju očuvanja sigurnosti, neporecivosti i privatnosti podataka. Životni ciklus biometrijskih rješenja. Preduvjet su znanja stečena na diplomskom studiju.	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	<p>Studenti koji polože ovaj predmet steći će sljedeća znanja i vještine:</p> <ul style="list-style-type: none"> • Razumijevanje metoda za biometrijsku identifikaciju • Načini mjerenja biometrijskih karakteristika • Znanja o tehnologijama za biometrijsku autentifikaciju • Razumijevanje ograničenja pojedinih metoda i tehnologija za biometrijsku autentifikaciju. • Projektiranje i evaluacija sustava za biometrijsku autentifikaciju • Razumijevanje pravnih, socijalnih i etičkih aspekata primjena ovih tehnologija. 	
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.	
Nastavne cjeline:	Naziv	Sati
	Uvod u biometrijsku autentifikaciju. Definicija problema. Zahtjevi na metode za autentifikaciju. Primjene.	2
	Temelji obrade i analize biometrijskih signala i slika.	3
	Temelji raspoznavanja biometrijskih uzoraka. Ekstrakcija značajki signala i slika. Klasifikacija uzoraka. Teorija detekcije. Mjere točnosti i pogrešaka metoda za autentifikaciju.	3
	Pregled metoda i tehnologija za biometrijsku autentifikaciju. Raspoznavanje otisaka prstiju.	3
	Raspoznavanje lica iz vidljivih i termografskih slika.	2
	Raspoznavanje na temelju slike šarenice i mrežnice oka. Raspoznavanje na temelju geometrije ruke i hoda.	2
	Raspoznavanje otiska dlana. Raspoznavanje rukopisa i potpisa.	2
	Autentifikacija na temelju govora. DNK autentifikacija.	2
	Sklopovlje za biometrijsku autentifikaciju. Čitači otisaka prstiju. Sustavi za raspoznavanje lica, irisa i retine. Skeneri potpisa. Pametne kartice s biometrijskim karakteristikama.	3
	Biometrijski standardi. ISO norme. NIST norme. BioAPI. Pravni, etički i socijalni aspekti primjena biometrijske autentifikacije.	3
	Primjene u gospodarstvu i državnim institucijama. Primjeri projekata. Životni ciklus biometrijskih rješenja.	2
	Prezentacije studentskih seminarskih radova.	3
Način polaganja:	Seminarski rad, usmeni ispit	
Literatura:	A. K. Jain, P. Flynn, A. Ross, " Handbook of Biometrics", Springer, 2007 J. R. Vacca, Biometric Technologies and Verification Systems, Butterworth-Heinemann, 2007 H. Wechsler, Reliable Face Recognition Methods: System Design, Implementation and Evaluation, Springer, 2006	
Semestar:	2	
Izvođenje na engleskom:	Da	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Primijenjena kriptografija	
Nositelji:	Prof. dr.sc. Marin Golub	
Opis:	Predmet upoznaje studenta sa suvremenom primijenjenom kriptografijom u mjeri i na način koji odgovara specijalistima informacijske sigurnosti. Izlažu se suvremene tehnike kriptografije i kriptanalize, mehanizmi za njihovu primjenu i posljedice u kritičnim sustavima. Primarni fokus je na aplikacijama i njihovu postojećem statusu sigurnosti. Glavne teme uz ostalo uključuju: dokazivu sigurnost, algoritme za simetrično i asimetrično kriptiranje, postupke autentifikacije, funkcije za izračunavanje sažetka poruke (hash), digitalni potpis, kriptografske protokole za razmjenu ključeva, infrastrukturu javnog ključa (PKI), kriptanalitičke tehnike kao što su linearna i diferencijalna kriptanaliza, vremenski napadi, zadržavanje sadržaja memorije i drugo. Na vježbama će studenti programski ostvariti neki kriptografski sustav. Na predavanjima i vježbama će se poticati rasprava o statusu postojećih kriptografskih tehnologija te o praktičnim iskustvima u odabranim kriptografskim aplikacijama. Preduvjet su znanja stečena na diplomskom studiju.	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	Studenti će biti osposobljeni identificirati kriptografske tehnologije, procijeniti njihov aktualni status glede sigurnosti i ranjivosti te predstaviti te koncepte za različite vrste korisnika i primjena.	
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.	
Nastavne cjeline:	Naziv	Sati
	Sigurnosni mehanizmi. Ugrožavanje sigurnosti. Vrste napada na sigurnost i sigurnosni zahtjevi.	1
	Simetrični kriptosustavi (DES, 3DES, DESX, IDEA). Kriptiranje toka podataka (A5, RC4). Napredni kriptosustavi (AES).	1
	Načini kriptiranja (ECB, CBC, CFB, OFB, CTR).	1
	Napadi na kriptosustave. Uvod u kriptanalizu. Linearna i diferencijalna kriptanaliza.	1
	Asimetrični kriptosustavi (RSA, digitalna omotnica). Dobrota RSA kriptosustava.	1
	Funkcije za izračunavanje sažetka poruke (MD5, SHA). Digitalni potpis. Zapečaćena digitalna omotnica.	1
	Vježbe: Primjena kriptografskih algoritama	9
	Autentifikacija u zatvorenim sustavima. Jednostrana i obostrana autentifikacija.	1
	Prijava za rad. Zaštita pristupanja pojedinim sredstvima – autorizacija.	1
	Autentifikacijski protokol Kerberos. Nedostaci Kerberos protokola.	1
	Digitalni certifikat. Dijelovi sustava PKI. X.509 certifikat i autentifikacijski protokoli.	1
	Sigurnosna zaštitna stijena. Protokoli za zaštitu podataka na otvorenim mrežama (SSL, TLS, SET).	1
	Vježbe: Sigurnosni protokoli	10
Način polaganja:	Seminar, pismeni i usmeni ispit	
Literatura:	B. Schneier, Applied Cryptography, 2nd edition, J. Wiley & Sons, 1996. R. Anderson, Security Engineering, J. Wiley & Sons, 2001. L.C.Washington, Elliptic Curves, Chapman & Hall/CRC, 2003	
Semestar:	1	
Izvođenje na engleskom:	Ne	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Računalna forenzika	
Nositelji:	Prof. dr. sc. Marijan Đurek	
Opis:	<p>ICT je posljednjih godina veoma napredovala i postala je sastavni dio radnog i privatnog životnog okruženja. Javljaju se novi oblici pohrane podataka koji predstavljaju poboljšanje u odnosu na nedavnu prošlost, ali otvaraju vrata i skupini ljudi koja te podatke može i želi zlouporabiti.</p> <p>Računalna forenzika je znanost koja se bavi, sakupljanjem, pretraživanjem, analizom te prezentacijom podataka prikupljenih s elektroničkih medija. Međutim, moralna i pravna dilema je do koje granice osoba koja zna i može pristupiti tuđim računalnim resursima to doista i smije činiti. Kada se ta granica prijeđe, krši se zakon i započinje istraga tijekom koje se vrlo često obavlja pretraga računalnih resursa, prisluškuju telefonski razgovori, presreću poruke Internetom i sl. U okviru zakonskih ovlaštenja posebno obučeni stručnjaci rade na otkrivanju i pohranjivanju na sigurni medij podataka od interesa za istragu, pišu izvješća o obavljenom poslu, svjedoče na sudu. Zato je potrebno poznavati metodologiju postupanja, načinu prikupljanja dokaza, analize prikupljenog materijala i prezentaciji rezultata istrage. Pri radu koriste se određena hardverska i softverska pomagala. Kada slučaj dođe na sud, rezultati istrage se prezentiraju odvjetnicima, sucu i poroti. Izuzetno je važno da forenzički stručnjak na jednostavan način prezentira rezultate kako bi ga svi mogli razumjeti jer njegova uloga može biti ključna u rješavanju zločina. Preduvjet su znanja stečena na diplomskom studiju.</p>	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	<p>Studenti koji polože ovaj predmet steći će sljedeća znanja i vještine:</p> <ul style="list-style-type: none"> • Razumijevanje uloge računalne forenzike u suvremenom okruženju računalnih i komunikacijskih tehnologija, • Upoznavanje s postupcima održavanja sigurnih računarskih sustava i poboljšanje tehnika zaštite računarskih sustava • Upoznavanje se računalnom etikom i legislativom. 	
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.	
Nastavne cjeline:	Naziv	Sati
	Uvod u računalnu forenziku	2
	Računalni dokazi i legislativa	2
	Zloporaba računalnih i komunikacijskih tehnologije u kriminalne namjene	1
	Protokoli postupanja i dokumentiranje postupaka	1
	Pretraživanje i prikupljanje dostupnih podataka	1
	Analiza prikupljenih informacija	1
	Priprema i publiciranje izvještaja	1
	Razvoj forenzičkih alata	1
	Softverski forenzički alati (ENCASE)	2
	Hardverski forenzički alati	2
	Pretraga osobnog računala	2
	Restauracija obnovljivih sadržaja na osobnom računalu	1
	Internet i zloporaba Interneta	2
	Elektronička pošta: praćenje putanje, restauracija zagubljene, oštećene ili obrisane pošte i privitaka	1
	Pretraga složenih računalnih sustava	2
	Pedofilski, pornografski i slični sadržaji	1
	Neautorizirano korištenje softvera	2
	Neautorizirano korištenje audiograma i videograma	2
	Čišćenje ostataka korištenja računala	1
	Računalni nametljivci (virusi, crvi,...) i restauracija napadnutih sadržaja	2
Način polaganja:	Seminarski rad, usmeni ispit.	
Literatura:	<p>Criss Posise, Kevin Mandia, Matt Pepe: Incident Response and Computer Forensics, Second Edition, McGraw-Hill, Inc. New York, USA, 2001.</p> <p>Waren G. Kruse, Jay . H. Heiser: Computer Forensics: Incident Response Essentials</p> <p>E. Eugene Schultz, Russell Shumway: Incident Response: A Strategic Guide to Handling System and Network Security, Sums Publishing, 2001.</p>	
Semestar:	2	
Izvođenje na engleskom:	Ne	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Sigurnosna arhitektura i tehnologije	
Nositelji:	Prof. dr. sc. Mario Kovač, doc.dr.sc. Hrvoje Mlinarić	
Opis:	Sve veća zavisnost o velikim i distribuiranim mrežnim sustavima ističe posljedice upada i kompromitiranja sustava. Takvi sustavi se suočavaju sa sigurnosnim prijetnjama koje postaju sve sofisticiranije u svojem djelovanju i opsegu. Arhitektura tih sustava mora uključiti sigurnosne sposobnosti koje se mogu nositi s tim prijetnjama. Te sposobnosti uključuju sigurnosne protokole, enkripciju i autentifikaciju. Razina sigurnosti mnogih kriptografskih algoritama u velikoj mjeri ovisi o načinima zaštite ključnih dijelova algoritama od neovlaštenog pristupa. Programske izvedbe u većini slučajeva ne omogućuju takvu zaštitu već je potrebno koristiti kombinacije programskih i sklopovskih rješenja. U okviru predmeta objasniti će se načela ostvarivanja viših razina sigurnosti korištenjem nekih karakterističnih tehnologija sklopovske zaštite poput pametnih kartica, sklopovskih sigurnosnih modula (hardware security module – HSM), povezivanja s ostalim biometrijskim modulima i sl.). Preduvjet su znanja stečena na diplomskom studiju.	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	Predmet će upoznati studente s načinima izvedbe sigurnosnih algoritama u nekim karakterističnim tehnologijama (poput pametnih kartica, sklopovskih sigurnosnih modula, povezivanja s biometrijskim modulima i sl.).	
Oblici provođenja nastave:	Predavanja, seminarski radovi studenata, vježbe na računalu.	
Nastavne cjeline:	Naziv	Sati
	Uvodne analize rizika korištenja programskih krypto rješenja	2
	Analiza i odvajanje algoritama prema računalnoj zahtjevnosti.	2
	Sigurnosna i zahtjevnosna analiza distribucije algoritama s naglaskom na sigurnosno kritične dijelove.	2
	Načini izvedbe sigurnosno kritičnih algoritama u zaštićenim okolinama.	2
	Primjer zaštićene okoline: pametna kartica.	2
	Analiza sigurnosti nekih tipova pametnih kartica na tržištu te analiza postojećih normi i platformi.	3
	Praktikum: krypto aplikacije na pametnoj kartici	3
	Primjer zaštićene okoline: HSM (hardware security module)	4
	Praktikum: algoritmi u okviru HSM-a	3
	Primjeri korištenja sklopovskih rješenja u tipičnim aplikacijama te usporedba sigurnosti	3
	Završni praktikum: sistemski pogled na programsku i sklopovsku krypto podršku	4
Način polaganja:	Seminarski rad, usmeni ispit	
Literatura:	Izabrani stručni članci i dokumentacija	
Semestar:	1	
Izvođenje na engleskom:	Da	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Sigurnost bežičnih mreža	
Nositelji:	Prof. dr. sc. Dina Šimunić	
Opis:	Bežični komunikacijski sustavi predstavljaju temelj poslovne i osobne komunikacije. Tehnologijska osnovica rada i primjena bežičnih mreža su raznovrsne prirode i doista impresivnog rasta. Stoga će se studenti tijekom izvođenja nastave upoznati s osnovama rada suvremenih bežičnih mreža, kao i izazovima aspekta sigurnosti ovih mreža. Predmet obuhvaća pregled rada napose fizičkog i pristupnog sloja suvremenih bežičnih mreža u raznovrsnoj poslovnoj i osobnoj uporabi, kao i zahtjeva za sigurnost i opasnostima u radu. Osim navedenog, važeće norme i zakonski akti ovog područja u svijetu i Republici Hrvatskoj, kao i različiti koncepti sigurnosti bežičnih mreža u različitim uvjetima primjene predstavljat će značajan dio grade predmeta. Budući da se bežične mreže kontinuirano i vrlo brzo razvijaju i nalaze sve veće primjene, predmet obuhvaća prezentaciju tehnologija i norma u nastajanju. Studentima će također biti razjašnjene ranjivost i protumjere ublažavanja i rješavanja problema sigurnosti bežičnih mreža različitih primjena. Na kraju, predviđeno je aktivno sudjelovanje studenata u izradi analize slučaja nekoliko tipova poslovnih mreža. Predviđet su znanja stečena na diplomskom studiju.	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	Student će biti osposobljen za izbor, oblikovanje i vrednovanje tehnološke infrastrukture u realizaciji sigurnih bežičnih mreža određen primjene uz zadovoljenje zakonskih propisa i izjava sigurnosnih politika.	
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.	
Nastavne cjeline:	Naziv	Sati
	Temelji i postojeće primjene bežičnih mreža	5
	Raščlamba bežičnih mreža	4
	Sigurnost fizičkog sloja	4
	Sigurnost pristupnog sloja	4
	Tehnologije i norme u nastajanju	4
	Tehničke protumjere	4
	Analiza slučaja poslovnih mreža	5
Način polaganja:	Seminarski rad, usmeni ispit.	
Literatura:	Yang Xiao, Xuemin Shen, Ding-Zhu Du (Eds), Wireless Network Security, 1st edition, Springer, 2007 John R. Vacca, Guide to Wireless Network Security, 1st edition, Springer, 2006 Levente Buttyan, Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, 1st edition, Cambridge University Press, 2008	
Semestar:	2	
Izvođenje na engleskom:	Da.	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Sigurnost elektroničkog poslovanja	
Nositelji:	Prof. dr. sc. Boris Vrdoljak, Prof. dr. sc. Vedran Batoš	
Opis:	<p>Zbog njegove sveprisutnosti Internet postaje uspješan medij za poslovanje. Glavne teme ovog kolegija odnose se na tehnološku infrastrukturu, aplikacije i politike sa stanovišta sigurnosti.</p> <p>Razumijevanje tehnologije Interneta je jako važno zbog oblikovanja poslovnih modela. Studenti će biti upoznati s tehnologijama koje realiziraju elektroničko poslovanje te s analizom nekih modela zanimljivih iz tehnološke perspektive. Glavni fokus bit će: na upoznavanju s WWW tehnologijama i trendovima, na Active Server Pages (ASP), na osnovama Extensible Mark Up Language (XML), na sustavima za elektroničko plaćanje te na problemima koji su vezani za autentifikaciju, sigurnost i privatnost. Kolegij pretpostavlja skromno poznavanje HTML-a. Nakon kratkog pregleda HTML-a studenti će pisati ASP skripte kako bi kreirali dinamički HTML i vezu na bazu podataka. Nakon toga bit će upoznati sa strukturom XML-a. Predmet pokriva i integraciju XML-a i ASP-a.</p> <p>Kroz kolegij bit će dan pregled aplikacija za elektroničko poslovanje u maloprodaji, sektoru državnih službi i zdravstvu. Ove aplikacije će prikazati elektroničko poslovanje tipa "consumer-business", "business-business" kroz fizičke i digitalne proizvode. Različiti poslovni modeli koji podupiru ove aplikacije bit će prikazani iz strateške i operativne perspektive. Kolegij će također dati pregled ključnih zakonskih obveza te problema vezanih na sigurnosnu politiku koja se odnosi na elektroničko poslovanje. To su naročito problemi koji se odnose na privatnost, odabir i ocjenu sadržaja te na intelektualna prava.</p> <p>Kao preduvjeti preporučaju se kolegij Sigurnost programske podrške i baza podataka te poznavanje programskog jezika C ili Java.</p>	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	Student će biti osposobljen za izbor, oblikovanje i vrednovanje kako tehnološke tako i aplikacijske infrastrukture u realizaciji poslovnih modela, uz zadovoljenje zakonskih propisa i izjava sigurnosnih politika.	
Oblici provođenja nastave:	Predavanja, vježbe i seminarski radovi.	
Nastavne cjeline:	Naziv	Sati
	Osnove elektroničkog poslovanja	3
	Platni i mikroplatni sustavi	3
	Poslovni modeli i kategorije	3
	Tehnologije i aplikacije za realizaciju e-poslovanja	4
	Zaštita transakcija	3
	Elektroničko plaćanje	3
	Kartično poslovanje	3
	Zakonske odredbe, privatnost i intelektualna prava	3
	Primjena elektroničkog poslovanja	5
Način polaganja:	Seminarski rad, usmeni ispit.	
Literatura:	<p>O'Mahoney, D., Peirce, M., Tewari, H., "Electronic Payment Systems for E-Commerce", Artech House Inc., Norwood, USA, 2001.</p> <p>Bidgoli, H., "Electronic Commerce Principles and Practice", Academic Press Inc., San Diego, USA, 2002.</p> <p>Hartmant, A., Sifonis, J. G., & Kador, J., 'Net Ready', McGraw-Hill, NY, USA, 2002.</p> <p>Odabrani članci i dokumentacija</p>	
Semestar:	2	
Izvođenje na engleskom:	Da.	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Sigurnost programske podrške i baza podataka																																																	
Nositelji:	Prof. dr. sc. Mirta Baranović, prof. dr. sc. Krešimir Fertalj																																																	
Opis:	<p>Loše projektiranje i izgradnja softvera predstavljaju glavni uzrok ranjivosti današnjeg softvera u primjeni. Što više, uz mobilnost koda kao realnosti današnjice, posebno u kontekstu Web tehnologija i upravljanja digitalnim pravima, projektanti sustava su suočeni sa zaštitom računala od izvanjskog softvera te od zaštitnog softvera koji izvode vanjska računala. U ovom kolegiju promatra se softver kao mehanizam za napad, kao alat za zaštitu resursa te kao na resurs koji treba zaštititi. Glavne teme uključuju: proces projektiranja softvera; izbor programskih jezika; operacijske sustave; baze podataka te platforme distribuiranih objekata za izgradnju sigurnih sustava; najčešće ranjivosti softvera kao što je "buffer overflow" i natjecanje za zadovoljenje uvjeta (race condition); reviziju softvera; dokazivanje svojstava softvera; označavanje softvera i podataka vodenim žigovima; zbudujući kod koji zavarava; neprobojni softver; te prednosti i dobitke otvorenog i zatvorenog razvoja programa.</p> <p>Sustavi za upravljanje bazama podataka su sveprisutni u današnjem društvu te su važan alat u podizanju njihove produktivnosti. Sposobnost uskladištenja, pristupa i upravljanja podacima u takvim sustavima postaje kritična za svaku organizaciju. Baze podataka se nalaze u centru strategije informacijskih sustava svake organizacije. Na svim razinama u organizaciji korisnici mogu očekivati da će imati kontakt sa sustavima za baze podataka. Stoga vještina u korištenju takvih sustava, njihovo razumijevanje u smislu sposobnosti i ograničenja, poznavanje kako pristupiti podacima izravno ili posredstvom tehničkih eksperata, poznavanje kako učinkovito koristiti informaciju koju ti sustavi osiguravaju te mogućnost projektiranja novih sustava i odgovarajućih aplikacija je značajna prednost i nužnost današnjice. Sustavi za upravljanje relacijskim bazama podataka (RDBMS) su danas u primjenama još uvijek dominantni te su jedan od glavnih fokusa predmeta. Preduvjet je poznavanje rada s relacijskim bazama podataka.</p>																																																	
ECTS:	6																																																	
Sati nastave:	30																																																	
Kompetencije:	Student će biti osposobljen za projektiranje i izgradnju sigurnog softvera, te za prepoznavanje ranjivosti postojećih aplikacija i njihovu zaštitu. Pored toga studenti će biti osposobljeni za vrednovanje sustava za upravljanje bazama podataka te za njihovu ispravnu ugradnju posebno s aspekta ostvarenja zahtjeva informacijske sigurnosti.																																																	
Oblici provođenja nastave:	Predavanja, seminarski radovi studenata.																																																	
Nastavne cjeline:	<table border="1"> <thead> <tr> <th>Naziv</th> <th>Sati</th> </tr> </thead> <tbody> <tr><td>Sigurnost programske podrške</td><td>2</td></tr> <tr><td>Statička analiza</td><td>1</td></tr> <tr><td>Upravljanje unosom podataka</td><td>2</td></tr> <tr><td>Buffer overflow</td><td>1</td></tr> <tr><td>Pogreške i iznimke</td><td>1</td></tr> <tr><td>Ugradnja sigurnosti u višeslojne aplikacije</td><td>2</td></tr> <tr><td>Sigurnost web aplikacija</td><td>2</td></tr> <tr><td>XML i web servisi</td><td>2</td></tr> <tr><td>Sigurnost u ERP sustavima</td><td>2</td></tr> <tr><td>Privilegirani programi</td><td>1</td></tr> <tr><td>Zakonski, socijalni i etički aspekti zaštite podataka</td><td>1</td></tr> <tr><td>Strategija i politike zaštite podataka</td><td>1</td></tr> <tr><td>Diskrecijska zaštita podataka</td><td>1</td></tr> <tr><td>Zaštita podataka temeljena na ulogama</td><td>1</td></tr> <tr><td>Kontekstno ovisna zaštita podataka</td><td>1</td></tr> <tr><td>Sigurnosne prijetnje, SQL injekcija, problem zaključivanja</td><td>2</td></tr> <tr><td>Uloga administratora podataka u zaštiti baze podataka, podjela uloga</td><td>1</td></tr> <tr><td>Nadgledanje rada korisnika</td><td>1</td></tr> <tr><td>Maskiranje podataka, šifriranje podataka</td><td>1</td></tr> <tr><td>Virtualna privatna baza podataka</td><td>1</td></tr> <tr><td>Baze podataka s višerazinskom zaštitom podataka</td><td>1</td></tr> <tr><td>Zaštita podataka u distribuiranim bazama podataka, skladištima podataka, integriranim heterogenim sustavima baza podataka</td><td>1</td></tr> <tr><td>Zaštita podataka u objektnim, multimedijским i XML bazama podataka.</td><td>1</td></tr> </tbody> </table>	Naziv	Sati	Sigurnost programske podrške	2	Statička analiza	1	Upravljanje unosom podataka	2	Buffer overflow	1	Pogreške i iznimke	1	Ugradnja sigurnosti u višeslojne aplikacije	2	Sigurnost web aplikacija	2	XML i web servisi	2	Sigurnost u ERP sustavima	2	Privilegirani programi	1	Zakonski, socijalni i etički aspekti zaštite podataka	1	Strategija i politike zaštite podataka	1	Diskrecijska zaštita podataka	1	Zaštita podataka temeljena na ulogama	1	Kontekstno ovisna zaštita podataka	1	Sigurnosne prijetnje, SQL injekcija, problem zaključivanja	2	Uloga administratora podataka u zaštiti baze podataka, podjela uloga	1	Nadgledanje rada korisnika	1	Maskiranje podataka, šifriranje podataka	1	Virtualna privatna baza podataka	1	Baze podataka s višerazinskom zaštitom podataka	1	Zaštita podataka u distribuiranim bazama podataka, skladištima podataka, integriranim heterogenim sustavima baza podataka	1	Zaštita podataka u objektnim, multimedijским i XML bazama podataka.	1	
Naziv	Sati																																																	
Sigurnost programske podrške	2																																																	
Statička analiza	1																																																	
Upravljanje unosom podataka	2																																																	
Buffer overflow	1																																																	
Pogreške i iznimke	1																																																	
Ugradnja sigurnosti u višeslojne aplikacije	2																																																	
Sigurnost web aplikacija	2																																																	
XML i web servisi	2																																																	
Sigurnost u ERP sustavima	2																																																	
Privilegirani programi	1																																																	
Zakonski, socijalni i etički aspekti zaštite podataka	1																																																	
Strategija i politike zaštite podataka	1																																																	
Diskrecijska zaštita podataka	1																																																	
Zaštita podataka temeljena na ulogama	1																																																	
Kontekstno ovisna zaštita podataka	1																																																	
Sigurnosne prijetnje, SQL injekcija, problem zaključivanja	2																																																	
Uloga administratora podataka u zaštiti baze podataka, podjela uloga	1																																																	
Nadgledanje rada korisnika	1																																																	
Maskiranje podataka, šifriranje podataka	1																																																	
Virtualna privatna baza podataka	1																																																	
Baze podataka s višerazinskom zaštitom podataka	1																																																	
Zaštita podataka u distribuiranim bazama podataka, skladištima podataka, integriranim heterogenim sustavima baza podataka	1																																																	
Zaštita podataka u objektnim, multimedijским i XML bazama podataka.	1																																																	
Način polaganja:	Seminarski rad, usmeni ispit																																																	
Literatura:	<p>B. Chest, J. West: Secure Programming with Static Analysis, Addison-Wesley Professional, 2007.</p> <p>The Art of Software Security Assessment: Identifying and Preventing M. Dowd, J. McDonald, J. Schuh: Software Vulnerabilities. Addison-Wesley Professional, 2006.</p> <p>B. Thuraisingham: Database and Applications Security: Integrating Information Security and Data Management, Auerbach, 2005.</p> <p>C. J. Date: Introduction to Database Systems, (8th Edition), Addison Wesley, 2004</p> <p>D. F. Ferraiolo, R. D. Kuhn, R. Chandramouli: Role-Based Access Control, (2th Edition) Artech House, Inc., 2007</p>																																																	
Semestar:	1																																																	
Izvođenje na engleskom:	Da																																																	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.																																																	

Predmet:	Ekonomski aspekti informacijske sigurnosti	
Nositelji:	Prof. dr. sc. Mario Spremić	
Opis:	<p>Informacijski sustavi predstavljaju okosnicu modernog poslovanja jer brzo i automatizirano provode poslovne transakcije i omogućuju efikasnije i konkurentnije poslovanje. Što se informacije i informacijski sustavi intenzivnije koriste u poslovanju, više je pozornosti potrebno posvetiti sustavnim mjerama kontrole, nadzora i provjere sigurnosti. Efikasni i djelotvorni informacijski sustavi se redovito trebaju podvrgavati unutarnjoj i vanjskoj reviziji, odnosno provjeri njihove učinkovitosti, pouzdanosti i sigurnosti. Razvoj sustava informacijske sigurnosti treba počivati na relevantnoj procjeni rizika i njihovu utjecaju na poslovanje, pri čemu pri razmatranju kontrolnih protumjera u obzir treba uzeti regulatorne, ekonomske, financijske, tehnološke, metodološke i ostale razloge. Upravo iz tih razloga problemu informacijske sigurnosti potrebno je pristupiti holistički i cjelovito, uz detaljnu ekonomsku analizu i procjenu ulaganja. Kao i kod bilo koje vrste ulaganja u informatiku, ulaganju u informacijsku sigurnost treba prethoditi detaljna ekonomska analiza uz studiju izvedivosti i dugoročno održivu strategiju.</p>	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	<p>Studenti će steći osnovna razumijevanja procjene važnosti sigurnosnih problema u informacijskim sustavima i njihova utjecaja na cjelokupno poslovanje. Studenti će steći metodološka i praktična znanja procjene razine informatičkih rizika, odnosno razine njihova utjecaja na cjelokupno poslovanje, što će im omogućiti planirati cjelovite strategije odgovora na rizike. Studenti bi trebali usvojiti znanja i vještine provedbe ekonomske analize i procjene isplativosti provedbe kontrolnih (zaštitnih) mjera, kao i znanja i vještine provjere (revizije) sustava informacijske sigurnosti. Studenti će steći znanja, vještine i praktična iskustva provjere (revizije, certificiranja) sustava informacijske sigurnosti prema najvažnijim svjetskim praksama, normama i standardima</p>	
Oblici provođenja nastave:	Predavanja, vježbe i seminarSKI radovi	
Nastavne cjeline:	Naziv	Sati
	Mehanizmi strateškog upravljanja informatikom (IT Governance) i uloga informacijske sigurnosti	2
	Vrste informatičkih sigurnosnih rizika	2
	Upravljanje informatičkim sigurnosnim rizicima i koraci i faze analize njihova utjecaja na poslovanje	4
	Metode i načini ekonomskog vrednovanja negativnog učinka informatičkih sigurnosnih rizika na poslovanje	4
	Određivanje prihvatljive razine rizika obzirom na poslovne ciljeve i zahtjeve, dodjela obveza i odgovornosti	2
	Izrada i provedba strategije i procjena isplativosti ulaganja u informacijsku sigurnost	2
	Ekonomska analiza opravdanosti i izvedivosti provedbe sigurnosnih kontrolnih protumjera	2
	Koraci i faze izrade plana odgovora na rizike	2
	Krovne i izvedene metodologije upravljanja informacijskom sigurnošću i prikaz njihove primjene u praksi (ISO 27000, CobiT, PCI DSS, Risk IT, ISM2, itd.)	2
	Provedba revizije informacijskih sustava, ekonomske koristi od certificiranja sustava informacijske sigurnosti	4
	Prikaz tijeka procesa certificiranja sustava informacijske sigurnosti	2
	Organizacijski aspekti informacijske sigurnosti (institucije i regulativa, hijerarhijski položaj voditelja informacijske sigurnosti)	2
Način polaganja:	Seminarski rad, usmeni ispit.	
Literatura:	<p>Panian, Ž., Spremić M. i suradnici (2007): Korporativno upravljanje i revizija informacijskih sustava, Zgombić i partneri, Zagreb, 2007</p> <p>Spremić, M. (2009): IT Governance and IT Risk Management Principles And Methods For Supporting "Always-On" Enterprise Information Systems, in a book Always-On Enterprise Information Systems for Business Continuance: Technologies for Reliable and Scalable Operation, IGI Publishing, ISBN: 978-1-60566-723-2, edited by Bajgoric, Nijaz.</p> <p>Spremić, M. (2011): Standards and Frameworks for Information System Security Auditing and Assurance, Proceedings of the World Congress on Engineering 2011 (WCE 2011). Newswood Limited. Part vol.1, 2011, 514-19. Hong Kong, China</p> <p>Spremić, M. (2011): Measuring IT governance maturity - evidences from using regulation framework in the republic Croatia, European Computing Conference. Proceedings of the European Computing Conference (ECC '11). WSEAS Press. 2011, 98-104. Athens, Greece.</p> <p>Hunton, J.E., Bryant, S.M., Bagranoff, N.A. (2004): Information technology Audit, John Wiley & Sons.</p>	
Semestar:	2	
Izvođenje na engleskom:	Da	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	

Predmet:	Pravni aspekti informacijske sigurnosti (predaje se od ak. god. 2012./2013.)	
Nositelji:	Prof. dr.sc. Dražen Dragičević	
Opis:	<p>Intenzivan znanstveno-tehnološki razvoj, od sredine prošlog stoljeća do danas, prate nastojanja nacionalnih zakonodavstava i međunarodnih organizacija da stvore takvo pravno okruženje u kojem će se daljnji informacijski razvoj nesmetano i sigurno odvijati.</p> <p>Pravna regulativa, okrenuta uređenju odnosa i propisivanju granica u fizičkom svijetu, našla se u problemima zbog čega su se zakonske promjene događale neujednačeno, sporo i selektivno i to ponajprije na onim područjima i onim redoslijedom kako su se zloporabe uočavale. Tako je šezdesete godine obilježio početak pravne regulacije na području zaštite osobnih podataka, sedamdesete pravna zaštita od gospodarskog računalnog kriminala, osamdesete zaštita intelektualnog vlasništva, dok je za devedesete svojstveno stvaranje i uspostava normativnog okvira regulacije elektroničkog trgovanja. Razvoj i sve šire korištenje elektroničkih komunikacija doveo je do novih odnosa kao i potrebe reguliranja prava i obveza kako korisnika tako i davatelja usluga informacijskog društva.</p> <p>U sklopu predmeta pratit će se zakonske promjene, postojeće pozitivno pravo i sudska praksa, kao i prijedlozi za uspostavu novog regulatornog okvira na područjima od interesa za uspostavu efikasne pravne infrastrukture informacijske sigurnosti.</p>	
ECTS:	6	
Sati nastave:	30	
Kompetencije:	<p>Studenti će steći osnovni uvid u razvoj pravne regulative na području zaštite osobnih podataka, računalnog kriminaliteta, zaštite intelektualnog vlasništva, normativnog okvira elektroničkog trgovanja i odgovornosti davatelja usluga informacijskog društva. Upoznat će se s relevantnim pravnim iskustvima iz Republike Hrvatske i Europske unije, posebno kroz primjere iz sudske prakse Suda EU i Europskog suda za ljudska prava, te kroz selektivnu komparativnu analizu propisa s posebnim osvrtom na hrvatsko pozitivno zakonodavstvo.</p>	
Oblici provođenja nastave:	Predavanja i seminarski radovi	
Nastavne cjeline:	Naziv	Sati
	Informacijske tehnologije i osobna prava	2
	Pravo i informacijsko-komunikacijske tehnologije	2
	Normativni i institucionalni okvir informacijske sigurnosti	2
	Informacijska i komunikacijska privatnost	4
	Konvencija o kibernetičkom kriminalitetu	4
	Implementacija Konvencije o kibernetičkom kriminalitetu u RH	2
	Visoke tehnologije i intelektualno vlasništvo	4
	Pravna zaštita softvera, baza podataka i internet domena	4
	Odgovornost davatelja usluga na Internetu	2
	Pravni okvir elektroničkog trgovanja	4
Način polaganja:	Seminarski rad, usmeni ispit.	
Literatura:	<p>"Pravna informatikai" (knjiga u pripremi), Narodne novine, Zagreb, 2012.</p> <p>Odabrani dijelovi iz pozitivnog prava RH i primjeri iz sudske prakse</p> <p>Različiti materijali i podaci dostupni na Internetu</p>	
Semestar:	2	
Izvođenje na engleskom:	Ne	
Način praćenja kvalitete:	Praćenje kvalitete i uspješnosti izvedbe predmeta sukladno sustavu upravljanja kvalitetom Sveučilišta u Zagrebu. Samovrednovanje nastave i anketiranje polaznika.	