

Studiju kursa apraksts**Kiberdrošības pamati un sistēmu aizsardzība pret kiberuzbrukumiem**

Kursa apraksta statuss: Apstiprināts

Kursa apraksta versija: 1.00

Kursa apraksta apstiprināšanas datums: 25.04.2024 11:30:17

Par studiju kursu			
Kursa kods:	SZF_145	LKI līmenis:	7. līmenis
ECTS:	6.00	Kredītpunkti:	4.00
Zinātnes nozare:	Tiesību zinātnes		
Mērķauditorija:	Tiesību zinātne; Civilā un militārā aizsardzība		
Studiju kursa vadītājs			
Kursa vadītājs:	Sanita Vīksne		
Studiju kursa īstenotājs			
Struktūrvienība:	Sociālo zinātņu fakultāte		
Vadītājs:	Karina Palkova		
Kontaktinformācija:	Dzirciema iela 16, Rīga, szf@rsu.lv		

Studiju kursa plānojums						
Pilns laiks						
Daļas nr.	Īstenošanas forma	Skaits	Ilgums (ak.st)	Kontaktstundas	Gala pārbaudījums	ECTS
1	Lekcijas	32	2	64	Eksāmens (Rakstisks)	6.00
	Nodarbības	8	2	16		
	Kopā:		80			
Nepilns laiks						
Daļas nr.	Īstenošanas forma	Skaits	Ilgums (ak.st)	Kontaktstundas	Gala pārbaudījums	ECTS
1	Lekcijas	32	2	64	Eksāmens (Rakstisks)	6.00
	Nodarbības	8	2	16		
	Kopā:		80			

Studiju kursa apraksts	
Priekšzināšanas:	
Sekmīgi apgūti iepriekšējos semestros realizētie studiju kursi.	
Mērķis:	
Iepazīstināt studējošos ar jaunākajām digitālo tehnoloģiju tendencēm, kiberdrošību, veidojot studējošajiem izpratni par personu un uzņēmumu informatīvo drošību un tās tiesisko nodrošinājumu, kā arī sagatavot speciālistus ar padziļinātām zināšanām informācijas sistēmu un datortīklu aizsardzībā pret kiberuzbrukumiem.	

Tēmu saraksts**Pilns laiks**

Nr.	Tēma	Īstenošanas forma	Skaitis (norises vieta)
1.	IKT drošības pamatprincipi, kiberdrošība. Iekšējie datu apstrādes aizsardzības noteikumi.	Lekcijas	2 (auditorija)
2.	Vispārīgā datu aizsardzības regula.	Lekcijas	2 (auditorija)
3.	Personas datu aizsardzības jēdziens, personas datu apstrādes principi un mērķi. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība.	Lekcijas	4 (auditorija)
4.	Personas datu aizsardzības speciālista funkcijas un pienākumi.	Lekcijas	2 (auditorija)
5.	Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums.	Lekcijas	2 (auditorija)
6.	Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. CSRF, XSS uzbrukumi, SQL injekcijas.	Lekcijas	4 (auditorija)
7.	Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. Videonovērošanas un telpu piekļuves kontroles sistēmas.	Lekcijas	2 (auditorija)
8.	Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti.	Lekcijas	2 (auditorija)
9.	Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati.	Lekcijas	2 (auditorija)
10.	Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes.	Lekcijas	2 (auditorija)
11.	Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. Interneta protokolu drošība, TCP, DNS un maršrutēšana.	Lekcijas	2 (auditorija)
12.	Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi.	Lekcijas	2 (auditorija)
13.	Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija	Lekcijas	2 (auditorija)
14.	Mākoņpakalpojumu un tīkla datu glabātuvju drošība gan no tehnisko, gan no juridisko aspektu viedokļa	Lekcijas	2 (auditorija)
15.	Netikete. Informācija, kā tiesiskās aizsardzības objekts.	Nodarbības	2 (auditorija)
16.	Kriminālatbildība un administratīvie pārkāpumi informatīvās drošības jomā.	Nodarbības	2 (auditorija)
17.	Drošības pasākumu plānošana, risku analīze. Nesankcionēta piekļuve informācijai, sociālā inženierija, konfidencialitāte.	Nodarbības	2 (auditorija)
18.	Personu un uzņēmumu īpašuma apdraudējuma veidi tīklā. Kiberdrošība gan, darbā gan mājās.	Nodarbības	2 (auditorija)
Kopā lekcijas			32
Kopā nodarbības			8
Kopā			40

Nepilns laiks			
Nr.	Tēma	Īstenošanas forma	Skaitis (norises vieta)
1.	IKT drošības pamatprincipi, kiberdrošība. Iekšējie datu apstrādes aizsardzības noteikumi.	Lekcijas	2 (auditorija)
2.	Vispārīgā datu aizsardzības regula.	Lekcijas	2 (auditorija)
3.	Personas datu aizsardzības jēdziens, personas datu apstrādes principi un mērķi. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība.	Lekcijas	4 (auditorija)
4.	Personas datu aizsardzības speciālista funkcijas un pienākumi.	Lekcijas	2 (auditorija)
5.	Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums.	Lekcijas	2 (auditorija)
6.	Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. CSRF, XSS uzbrukumi, SQL injekcijas.	Lekcijas	4 (auditorija)
7.	Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. Videonovērošanas un telpu piekļuves kontroles sistēmas.	Lekcijas	2 (auditorija)
8.	Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti.	Lekcijas	2 (auditorija)
9.	Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati.	Lekcijas	2 (auditorija)
10.	Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes.	Lekcijas	2 (auditorija)
11.	Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. Interneta protokolu drošība, TCP, DNS un maršrutēšana.	Lekcijas	2 (auditorija)
12.	Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi.	Lekcijas	2 (auditorija)
13.	Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija	Lekcijas	2 (auditorija)
14.	Mākoņpakalpojumu un tīkla datu glabātuvju drošība gan no tehnisko, gan no juridisko aspektu viedokļa	Lekcijas	2 (auditorija)
15.	Netikete. Informācija, kā tiesiskās aizsardzības objekts.	Nodarbības	2 (auditorija)
16.	Kriminālatbildība un administratīvie pārkāpumi informatīvās drošības jomā.	Nodarbības	2 (auditorija)
17.	Drošības pasākumu plānošana, risku analīze. Nesankcionēta piekļuve informācijai, sociālā inženierija, konfidencialitāte.	Nodarbības	2 (auditorija)
18.	Personu un uzņēmumu īpašuma apdraudējuma veidi tīklā. Kiberdrošība gan, darbā gan mājās.	Nodarbības	2 (auditorija)
Kopā lekcijas			32
Kopā nodarbības			8
Kopā			40

Vērtēšana

Patstāvīgais darbs:

Studējošie patstāvīgi gatavojas nodarbībām, lasot un analizējot docētāja piedāvātos materiālus, analizējot nepieciešamo informāciju, kā arī analizējot ierīču, programmnodrošinājuma un sistēmu iespējas (skat. Obligāto literatūru un papildus izmantojamo informācijas avotu sarakstu), lasa docētāja papildus piedāvāto literatūru, pilda docētāja sagatavotos uzdevumus.

Lai izvērtētu studiju kursa kvalitāti kopumā, studentam jāaizpilda studiju kursa novērtēšanas anketa Studējošo portālā.

Vērtēšanas kritēriji:

Nodarbību apmeklējums vismaz 60% no kopējā nodarbību skaita (100%)

Noslēguma pārbaudījums – Diferencēts pārbaudījums, kas tiek īstenots testa veidā.

Tests satur 30-40 jautājumu ar vairākiem atbildes variantiem.

Gala pārbaudījums (pilna laika studijas):

Eksāmens (Rakstisks)

Gala pārbaudījums (nepilna laika studijas):

Eksāmens (Rakstisks)

Studiju rezultāti

Zināšanas:

1. Pārzin kiberdrošības pamatus, drošību internetā un digitālo ierīču un tīkla kiberhigiēnu.
2. Pārzin tīkla etiķeti (netiķeti), digitālo saziņas līdzekļu izmantošanas kultūru.
3. Pārzin personas datu apstrādes tiesiskuma aspektus, Latvijas un Eiropas regulējumu personas datu apstrādes jomā.
4. Pārzin dažādus uzbrukumu veidus, tai skaita sociālas inženierijas pamatus.
5. Pārzin informācijas sistēmu, operētājsistēmu drošības pārvaldības labas prakses principus.
6. Pārzin kriptogrāfijas pamatus un internetā pielietotās informācijas šifrēšanas tehnoloģijas.
7. Pārzin datortīkla drošības pamatus: drošības savienojuma izveide, droša lietotāju autentifikācija (t.sk. divfaktoru autentifikācija).
8. Pārzin videonovērošanas un telpu piekļuves kontroles sistēmu īpatnības, uzstādīšanas un uzturēšanas pamatprincipus.

Prasmes:

1. Prot pielietot zināšanas par kiberdrošības un personas datu aizsardzības aspektiem ikdienas dzīvē.
2. Prot identificēt veidus, kā aizsargāt personas datus no trešajām personām, t.sk., izmantojot digitālas drošības tehnoloģijas.
3. Prot veikt informācijas sistēmu drošības auditu un sistēmas drošības risku analīzi.
4. Prot identificēt CSRF, XSS, DoS, DDos uzbrukumus, SQL injekcijas, kā arī zina, kā aizsargāt IKT sistēmas no tiem.
5. Prot veikt organizācijās darbinieku apmācības par kiberdrošības pamatiem un ikdienas kiberhigienas nepieciešamību.
6. Prot veikt datu un sistēmu šifrēšanu, lai nodrošināt informācijas konfidencialitāti.

Kompetences:

Iekļaujas diskusijās par personu un uzņēmumu informatīvo drošību, kiberdrošību, prot atpazīt digitālās transformācijas darbā.

Bibliogrāfija

Obligātā literatūra:

Nr.	Nosaukums	Saite
1.	Ross J. Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems". 2008.	Saite
2.	Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone. "Computer Security Incident Handling Guide".	Saite
3.	Uldis Miķelsons. Informācijas sistēmu drošība. (latviešu plūsmai)	Saite
4.	Elektronisko dokumentu likums/Electronic Documents Law	Saite

5.	Fizisko personu datu apstrādes likums/Personal Data Processing Law	↗
6.	Vispārīgā datu aizsardzības regula/General Data Protection Regulation	
Papildu literatūra:		
Nr.	Nosaukums	Saite
1.	"E-pakalpojumi Latvijā Preces un pakalpojumi internetā". 2015. (latviešu plūsmai)	↗
2.	"Vēstuļu rakstīšanas VADLĪNIJAS". Valsts kanceleja, 2017. (latviešu plūsmai)	↗
3.	Informācijas sistēmu drošības pārbaudes vadlīnijas (VARAM). (latviešu plūsmai)	
4.	Personas datu apstrādes sistēmu audita rokasgrāmata. (latviešu plūsmai)	↗
Citi informācijas avoti:		
Nr.	Nosaukums	Saite
1.	Latvijas Drošāka interneta centrs – Sadaļa "Jaunami" (latviešu plūsmai)	↗
2.	Esidross.lv - vietne, kurā apkopota noderīga informācija tiem, kam rūp sava un sava datora, telefona vai citu viedierīču drošība internetā. – Sadaļa "Aktivitātes" (latviešu plūsmai)	↗
3.	Latvijas Drošāka interneta centrs – Sadaļa "Materiāli" (materiālu bibliotēkā) (latviešu plūsmai)	↗
4.	CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija) struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā IT drošības likuma ietvaros. – Sadaļa "Ziņas" (latviešu plūsmai)	↗