RTU studiju kurss "Informācijas drošība un privātums"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0828
Nosaukums	Informācijas drošība un privātums
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācībspēks	Rūta Pirta - Doktors, Docents
Apjoms daļās un kredītpunktos	1 daļa, 6.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Informācijas drošība ir uzņēmuma un personas datu un digitālās identitātes aizsargāšana. Tā ir viena no uzņēmumu stratēģiskajām spējām to nepārtrauktas darbības nodrošināšanai. Studiju kursā tiek apgūta riskos balstīta informācijas un personas datu aizsardzība, informācijas drošības pārvaldības un personas datu apstrādes procesi un veicamie pasākumi informācijas aizsardzībai.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir sniegt zināšanas un prasmes par informācijas drošību un personas datu aizsardzību uzņēmuma nepārtrauktas darbības nodrošināšanai un mērķu īstenošanai. Studiju kursa uzdevumi ir: 1. Radīt izpratni par informācijas drošības galvenajiem jēdzieniem. 2. Veidot informācijas klasifikācijas prasmes (informācijas drošības kontekstā). 3. Veidot informācijas drošības apdraudējumu un ievainojamību identificēšanas prasmes. 4. Veidot IT resursu risku un trešo pušu risku analīzes prasmes. 5. Veidot biznesa nepārtrauktības plānošanas prasmes. 6. Veidot incidentu pārvaldības prasmes. 7. Radīt izpratni par kriminalistikas (forensics) procesiem un metodēm, 8. Radīt izpratni par informācijas drošības pārvaldības metodoloģijām un standartiem un veidot IT kontroļu definēšanas prasmes. 9. Radīt izpratni par personas datu aizsardzības galvenajiem jēdzieniem, procesiem un regulējošajiem normatīvajiem aktiem. 10. Veidot nepieciešamo pasākumu definēšanas prasmes personas datu aizsardzībai uzņēmuma IT kontroles vidē.
Patstāvīgais darbs, tā organizācija un uzdevumi	Studiju kursa laikā studentiem ir jāizstrādā patstāvīgais uzdevums par informācijas drošības pārvaldības procesu izveidi un simulēšanu parauguzņēmumā: informācijas klasifikācija, IT resursu risku novērtējums, trešo pušu riski novērtējums, biznesa ietekmes analīze, biznesa nepārtrauktības plānošana, incidenta reaģēšana un izmeklēšana, piemērojot kriminālistikas metodes, personas datu kartēšana, personas datu ietekmes analīze (DPIA). Lekciju laikā tiek izskatītas patstāvīgā darba īstenošanai nepieciešamās metodes un tiks uzsākta praktiskā darba izpilde.
Literatūra	Obligātā. / Obligatory: Michael E. Whitman, Herbert J. Mattord. Principles of Information Security 6th Edition Cengage Learning, 2019 Michael E. Whitman, Herbert J. Mattord. Management of Information Security 6th Edition Cengage Learning, 2019 Starptautiskā standartizācijas organizācija (ISO). Standarts LVS ISO/IEC 27001:2017 "Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības" 2017 Starptautiskā standartizācijas organizācija (ISO). Standarts LVS ISO/IEC 27002:2017 "Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības prakses kodekss" 2017 Eiropas datu aizsardzības kolēģija. Eiropas datu aizsardzības kolēģijas rekomendācijas "Vispārējā datu aizsardzības regula: vadlīnijas, rekomendācijas, labākās prakses piemēri" 2018-2023 Guide to computer forensics and investigations / by Bill Nelson ... [et al.]. Boston, Mass. : Thomson Course Technology, c2006., xxvii, 643 lpp. : il. + 1 DVD-ROM. Papildu . / Additional: Informācijas drošības forums (ISF). Informācijas drošības foruma (ISF) metodiskie materiāli - https://www.securityforum.org/ 2012-2023 Eiropas Tīkla un informācijas drošība aģentūra (ENISA). Eiropas Tīkla un informācijas drošība aģentūras (ENISA) metodiskie materiāli - https://www.enisa.europa.eu/ 2012-2023 Howard, Doug.. Security 2020 : Reduce Security Risks This Decade [elektronisks resurss] /D.Howard, K.Prince, B.Schneier Hoboken : Wiley, 2010., 335 p. Informācijas sistēmu audita un kontroļu asociācijas (ISACA). Informācijas sistēmu audita un kontroļu asociācijas (ISACA) metodiskie materiāli - https://www.isaca.org/resources 2012-2023 Latvijas Republikas Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāts. Informācijas sistēmu drošības pārvaldības ieviešanas vadlīnijas 2008 Pirta-Dreimane, R., Brilingaite, A., Roponena, E., Parish, K., Grabis, J., Lugo, R.G., Bonders, M.. . CyberEscape approach to advancing hard and soft skills in cybersecurity education Proc. of the 25th HCI International Conference, July 2023 (LNCS series), Springer. p. 19.

Nepieciešamās priekšzināšanas	Zināšanas par informācijas drošības un risku pārvaldības pamatelementiem, tīmekļa vidē bāzētas programmatūras izmantošanas pamatprasmes.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Informācija un informācijas drošība.	4	6	0	0
Informācijas drošības pārvaldība, informācijas drošības pārvaldības procesi.	8	12	0	0
Informācijas drošības risku analīze - IT resursu riski, trešo pušu riski.	8	10	0	0
Biznesa nepārtrauktības pārvaldība - biznesa ietekmes analīze, biznesa nepārtrauktības un rezerves atjaunošanas plānošana.	8	10	0	0
Incidentu pārvaldība - gatavošanās incidentam, incidentu noteikšana un analīze, incidenta atklāšana, apturēšana un pēc incidenta aktivitātes.	6	12	0	0
Kriminālistikas (forensics) metodes.	4	8	0	0
Informācijas drošības pārvaldības metodikas un standarti (ISO 27000 grupa u.c.).	8	12	0	0
Informācijas drošības pārvaldības rīki.	4	6	0	0
Personas dati, to apstrāde, aizsardzība un pārvaldība.	6	10	0	0
IT veicamie pasākumi un kontroles personas datu aizsardzībai.	8	10	0	0
Kopā:	64	96	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Izprot informācijas drošības un personas datu aizsardzības galvenos jēdzienus.	Tests un eksāmens (zināšanu pārbaudes testa formā). Testi iekļaus teorētiskos un praktiskos uzdevumiem. Lai veiksmīgi nokārtotu testus, ir jāatbild pareizi uz vismaz 70% jautājumu.
Spēj klasificēt informāciju.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.
Spēj analizēt informācijas drošības riskus – spēj identificēt un novērtēt IT resursu riskus un trešo pušu riskus.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.
Spēj plānot biznesa nepārtrauktību, veikt biznesa ietekmes analīzi un plānot IT darbības atjaunošanu.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.
Spēj identificēt, klasificēt, analizēt, novērst un komunicēt informācijas drošības incidentu.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.
Izprot kriminālistikas (forensics) metodes un spēj tās piemērot informācijas drošības incidenta izmeklēšanā.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.
Izprot informācijas drošības un personas datu aizsardzības pārvaldības metodoloģijas, regulējošos normatīvos aktus un piemērojamos standartus (ISO 27000 grupa u.c.).	Tests un eksāmens (zināšanu pārbaudes testa formā). Testi iekļaus teorētiskos un praktiskos uzdevumiem. Lai veiksmīgi nokārtotu testus, ir jāatbild pareizi uz vismaz 70% jautājumu.
Spēj definēt un ieviest galvenos nepieciešamos pasākumus personas datu aizsardzībai uzņēmuma IT kontroles vidē.	Praktiskie darbi nodarbībās. Individuālie un grupas darbi.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Praktiskais darbs (individuāli un grupās)	40
Tests	10
Eksāmens	50
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	6.0	16.0	48.0	0.0		*	