

STUDIJU KURSA APRAKSTS

Studiju kursa nosaukums	Līderība	
Programma	Kiberdrošības pārvaldība	
Studiju gads	1.	
Akadēmiskais gads	2022/2023	
Studiju līmenis	2. cikls, maģistra studiju programma	
Studiju kursa kods	MKP014	
Studiju kursa docētājs	L.Peiseniece	
Kursa apjoms	2 KP vai 3 ECTS	
Modulis	Vadībzinību	
Studiju īstenošanas valoda	Angļu un latviešu	
Semestris, kad kurss tiek īstenots	1.,2.	
Studiju kursa īstenošanas veids	Klātiešana vai tiešsaiste	
Kursa īstenošanas mērķis	Sniegt studentiem teorētisku un praktisku izpratni par ilgtspēju, līderību un atbildīgu uzņēmējdarbību, uzsverot līderību kā sadarbību starp līderi un organizācijas darbiniekiem. Attīstīt zināšanas par informācijas nodrošināšanu, kā arī iegūt skaidru izpratni par to, kā ētiski vadīt, sazināties un veikt izmaiņas tehniskajās nodaļās un organizācijās. Raksturot līdera atbildību par darbinieku profesionālā radošā potenciāla atraisīšanu, kas vērsts uz organizācijas mērķu sasniegšanu.	
Prasības studiju kursa apguves uzsākšanai	IKT zināšanas un prasmes, prasme diskutēt un argumentēt savu viedokli, prezentāciju prasme.	
Studiju kursa saturs	Līderības lomas un funkcijas; Cilvēkfaktors kiberdrošībā; Līderība kibervidē Līderības izaicinājumi; Trešā līmeņa vadība: vērtību, pieņemumu, uzskatu un cerību analīze; Sociālās inženierijas ietekme; virtuālo organizāciju vadīšana dažādās kultūrās.	
Studējošo patstāvīgā darba organizācija un uzdevumi / Plānotās studiju formas un mācīšanas metodes	Students apmeklē lekcijas, piedalās semināros un situāciju analīžu diskusijās, izstrādā un prezentē patstāvīgo un grupu praktiskos darbus.	
	Studiju metodes	Studenta darba apjoms (h)
	Lekcijas	16
	Rakstisks grupas darbs	8
	Seminārs	16
	Praktiskais darbs individuāli	24
	Patstāvīgas studijas	16
	80 stundas	
Plānotie studiju rezultāti (zināšanas, prasmes, kompetences)	Spēja novērtēt un attīstīt personīgās līderības modeli. Prot organizēt multi-kultūras komandas darbu. Spēja saskatīt nepieciešamību un iespējas indivīda attīstībai līderībā un virzīt savu kompetenču pilnveidei, pamatojoties uz attiecīgajiem zinātnes, sociālajiem un ētikas aspektiem.	

	<p>(z1) Zina un izprot informācijas drošības pārvaldības jautājumus un to ietekmi uz uzņēmuma/organizācijas, konkurētspēju, attīstību, stabilitu un ilgtspējīgu darbību;</p> <p>(p5) Prot sadarboties, komunicēt, konsultēt, skaidrot un argumentēt informācijas drošības pārvaldības mērķus un rezultātus ieinteresētajām pusēm (speciālistiem un nespeciālistiem);</p> <p>(k6) Spēj noteikt un prognozēt mācību vajadzības, integrēt dažādu jomu zināšanas, dot ieguldījumu jaunu zināšanu radīšanā;</p> <p>(k8) Spēj izstrādāt, plānot, uzraudzīt informācijas aizsardzības pasākumus, gan procesu, gan tehnoloģiju, gan cilvēku uzvedības līmeņos, nodrošinot pasākumu efektivitāti.</p>			
Studiju kursu kalendārais plāns	1.nodarbība	Līderības lomas un funkcijas;		
	2.nodarbība	Cilvēkfaktors kiberdrošībā; Līderība kibervidē.		
	3.nodarbība	Līderības izaicinājumi; Trešā līmeņa vadība: vērtību, pieņemumu, uzskatu un cerību analīze;		
	4.nodarbība	Sociālās inženierijas ietekme; virtuālo organizāciju vadīšana dažādās kultūrās.		
Studiju rezultātu vērtēšanas metodes un kritēriji	<i>Studiju rezultāti</i>			
		1.	2.	3.
	<i>Pārbaudes forma</i>			
	<i>Rakstisks darbs auditorijā</i>	●		
	<i>Patstāvīgs darbs un tā prezentācija</i>	●	●	●
	<i>Rakstisks eksāmens</i>	●		●
Obligātā un papildliteratūra	<p>Obligātā literatūra: James.G.Clawson. Level Three Leadership: Getting Below the Surface Third Edition (Clawson, Pearson Prentice-Hall, 2010) Harvard Business Publishing Case Packet</p> <p>Papildliteratūra: Hadrnagy, C., (2011). Social Engineering: The Art of Human Hacking, NY, Wiley Cialdini, R. (2008). Influence: Science and practice, (5th ed.). NY: Prentice Hall The Feeling and Reality of Security (Bruce Schneier). www.schneier.com/blog/archives/2008/04/the_feeling_and_1.html Social engineering - exploiting human vulnerabilities. www.social-engineer.org</p>			
Rekomendējamie izvēles kursa elementi	Tiek saskaņots uzsākot studiju kursu			