STUDIJU KURSA APRAKSTS

Studiju kursa nosaukums	**Kiberdrošība un Kritiskās infrastruktūras aizsardzība**
Programma	Kiberdrošības pārvaldība
Studiju gads	1., 2.
Akadēmiskais gads	2022/2023
Studiju līmenis	2. cikls, maģistra studiju programma
Studiju kursa kods	MKP010
Studiju kursa docētājs	N.Komninos, A. Ambults
Kursa apjoms	4 KP vai 6 ECTS
Modulis	Kiberdrošība
Studiju īstenošanas valoda	Angļu un latviešu
Semestris, kad kurss tiek īstenots	2., 3.
Studiju kursa īstenošanas veids	Klātiene vai tiešsaiste
Kursa īstenošanas mērķis	Studiju kursa mērķis ir veidot padziļinātu izpratni par kiberdrošības dimensijām, līmeņiem, veiksmes faktoriem, kas nepieciešami uzņēmuma resursu aizsardzībai.
Prasības studiju kursa apguves uzsākšanai	-
Studiju kursa saturs	Kritiskās infrastruktūras pamatjēdzieni un taksonomija; Kritiskās infrastruktūras darbības stratēģijas, standartu, koncepciju un politikas dokumentu analīze; Datu centru drošības aspekti; Viedie tīkli, viedās tehnoloģijas un to drošības prasības.
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
Lekcijas	15%
Semināri	5%
Patstāvīgs, praktiskais darbs	40%
Praktiskais Darbs grupās	20%
Patstāvīgas studijas	20%
	160 stundas

Plānotie studiju rezultāti (zināšanas, prasmes, kompetences)	(z2) Īstenojot informācijas drošības pārvaldību, zina un prot patstāvīgi pielietot informācijas drošības rīkus, metodes, jaunākos atklājumus un inovācijas, uzņēmuma/organizācijas kritisko resursu aizsardzībai; (p3) Prot patstāvīgi identificēt un kritiski analizēt ar kiberdrošību saistītos riskus, noteikt, plānot un uzraudzīt sasniedzamo rezultātu risku mazināšanai; (k9) Spēj patstāvīgi formulēt un kritiski novērtēt esošos rezultatīvos rādītājus un plānot sasniedzamos biznesa nepārtrauktības procesu nodrošināšanā.

Studiju kursu kalendārais plāns	1.nodarbība	Kritiskās infrastruktūras pamatjēdzieni un taksonomija
	2.nodarbība	Kritiskās infrastruktūras darbības stratēģijas, standartu, koncepciju un politikas dokumentu analīze
	3.nodarbība	Datu centru drošības aspekti;
	4.nodarbība	Viedie tīkli, viedās tehnoloģijas un to drošības prasības.

Studiju rezultātu vērtēšanas metodes un kritēriji	*Studiju rezultāti* *Pārbaudes forma*	1.	2.	3.
	Patstāvīgs darbs auditorijā	●	●	●
	Grupas darbs auditorijā		●	●
	Patstāvīgs darbs un tā prezentācija		●	●
	Rakstisks eksāmens	●	●	●
Obligātā un papildliteratūra	Obligātā literatūra: Science of Cyber-Security - http://www.fas.org/irp/agency/dod/jason/cyber.pdf Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation - http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET%282011%29433828_EN.pdf Critical Infrastructure Protection standart family - http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx CIP-003-5 — Cyber Security — Security Management Controls: - http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-003-5&title=Cyber%20Security%20-%20Security%20Management%20Controls&jurisdiction=null NIST Releases Cybersecurity Framework Version 1.0 - http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm Papildu: National Cyber Security Strategies - http://www.gns.gov.pt/media/1238/ENISANationalCyberSecurityStrategies.pdf http://policyreview.info/articles/analysis/europe%E2%80%99s-fragmented-approach-towards-cyber-security			
Rekomendējamie izvēles kursa elementi	Tiek saskaņots uzsākot studiju kursu			