

RTU studiju kurss "Digitālās vides ētika, tiesības un kibernetika"**OL000 Liepājas akadēmija****Vispārējā informācija**

Kods	LA1544
Nosaukums	Digitālās vides ētika, tiesības un kibernetika
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācītspēks	Maija Demitere - Doktors, Docents
Mācītspēks	Kaspars Vārpiņš - Docents
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kurss iepazīstina ar digitālās vides tiesiskajiem un ētiskajiem aspektiem, kā arī kibernetikas principiem. Studenti apgūs prasmes kritiski analizēt tehnoloģiju izmantošanu un pielietot tiesiskos un drošības standartus izglītības vidē.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir attīstīt studentu spēju izprast un kritiski izvērtēt digitālās vides tiesiskos, ētiskos un kibernetikas aspektus, kā arī pielietot tos izglītības praksē. Studiju kursa uzdevumi: - izveidot prasmes analizēt un izprast digitālās vides tiesiskā regulējuma nostādnes un to pielietošanu praksē; - izvērtēt tehnoloģiju izmantošanas radītās ētikas problemātiku un risinājumus, pilnveidojot prasmes identificēt un risināt ētiskos jautājumus, kas saistīti ar datu izmantošanu, mākslīgo intelektu un digitālo vidi; - apskatīt kibernetikas pamatprincipus; - attīstīt prasmes kritiski analizēt digitālās vides un izaicinājumus un definēt atbildīgas un drošas rīcības pieejas; - iemācīt izvērtēt digitālo tehnoloģiju, operētājsistēmu un lietojumprogrammu izmantošanas iespējas un drošības aspektus izglītībā; - attīstīt prasmi izvērtēt datu avotu uzticamību, analizēt digitālās vides riskus un pieņemt pamatotus lēmumus.
Patstāvīgais darbs, tā organizācija un uzdevumi	Patstāvīgā darba temati un uzdevumi: 1. Reālu situāciju analīze (atbildīga darbība digitālajā vidē, ētiskas dilemmas tehnoloģiju izmantošanā). 2. Grupas projekts - draudu veidu atpazīšana, aizsardzības mehānismu un incidentu vadības raksturošana. 3. Interaktīva spēle - izstrādāt un novadīt interaktīvu spēli vai simulāciju kursabiedriem vai citai auditorijai, kurā tiek risinātas ētiskas dilemmas digitālajā vidē. Temata izvēle, scenārija izstrāde, spēles vadīšana un dalībnieku izvēles analīze. 4. Digitālo pēdas analīze – pašanalīzes veikšana par savu digitālo pēdu (kādi dati par sevi ir publiski pieejami, kā tos varētu samazināt vai aizsargāt, risku analīze). Personīgās digitālās drošības plāna izstrāde.
Literatūra	Obligātā/Obligatory: 1. Barkāne, I. (2023). Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai. Rīga: LU Akadēmiskais apgāds. https://www.apgads.lv/fileadmin/user_upload/lu_portal/apgads/izdevumi/2023/Barkane-Cilvektiesibu_nozime.pdf 2. Potapovs, M., & Kanasta, K.E. (Eds.). (2025). Cybersecurity in Latvia: Forging Resilience amidst Emerging Threats (1st ed.). Routledge. https://doi.org/10.4324/9781003638858 Pieejama: https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003638858/cybersecurity-latviamihails-potapovs-kate-kanasta 3. EKPI: Eiropas kibernetikas prasmju ietvars latviešu valodā - source/ekpi-eiropas-kibernetikasprasmju-ietvars-latviesu-valoda/"as-kibernetikasprasmju-ietvars-latviesu-valoda/ (EKPI kibernetikas speciālistu lomu profili un EKPI lietotāja rokasgrāmata) 4. European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 5. CERT.LV. Kiberincidentu novēršanas institūcija (2025). https://cert.lv 6. Fizisko personu datu apstrādes likums. (2018). https://likumi.lv/ta/id/300099-fizisko-personudatu-apstrades-likums 7. Autortiesību likums. (2000). https://likumi.lv/ta/id/5138-autortiesibu-likums 8. Vispārējā datu aizsardzības regula. (2016). https://eurlex.europa.eu/eli/reg/2016/679/oj/?locale=LV 9. Latvijas kibernetikas stratēģija 2023.-2026. gadam https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kibernetika%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf Papildu/Additional: 1. Krimināllikums (1999). https://likumi.lv/ta/id/88966-kriminallikums 2. Elektronisko sakaru likums. (2022). https://likumi.lv/ta/id/334345-elektronisko-sakaru-likums 3. Word Press. Esidrošs. (2025). https://www.esidross.lv/ 4. CERT.LV. DNS Ugunsgrāvis. (2025). https://dnsmuris.lv/ 5. Cisco. Open DNS. https://www.opendns.com/ 6. E-pasta datu noplūdes pārbaude - https://haveibeenpwned.com/
Nepieciešamās priekšzināšanas	Priekšzināšanas nav nepieciešamas.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
1. Digitālās vides tiesiskais un ētiskais pamats Digitālās vides tiesiskais regulējums. Autortiesības, informācijas brīvība un atbildība par saturu. Digitālās vides ētiskie izaicinājumi: MI izmantošana, datu komercializācija, izglītības vidē. Digitālo tehnoloģiju izmantošanas ētika un drošība izglītībā (mācību platformas, e-klases, Zoom, LMS u.c.) Digitālā pēda (Digitālais nospiedums) Digitālā higiēna un digitālā labbūtība: Uzmanības ekonomika un atkarību veicinošs tehnoloģiju dizains. Digitālās labbūtības ietvari (ES iniciatīvas)	4	12	0	0
2. Datortīklu un operētājsistēmu pamati kiberdrošībā Operētājsistēmu izmantošana Droša datortīkla izmantošana	4	12	0	0
3. Datu aizsardzība Riski, draudi, praktiski rīki datu un sistēmu aizsardzībā. Praktiski uzdevumi/piemēri par datu aizsardzību. Paroļu pārvaldīšana (uzticamas un neuzticamas metodes) un uzlaušana. Datu turēšana mākonī. Atvērtas/publiskas mapes izmantošanas riski Google Drive, OneDrive un citās platformās. IoT un viedierīču drošība. GDPR CERN Ļaunprogrammatūra	8	12	0	0
4. Interneta, mājaslapu un mobilo lietotņu darbība Lietotņu darbība. Datu uzglabāšana. Atļauju piešķiršana lietotnei. Mājaslapu sīkdatnes (angļu val. cookies). Interneta meklētāju darbība un meklēšana, izmantojot MI aģentus, to salīdzinājums. MI aģentu aizspriedumi (angļu val. bias).	4	12	0	0
5. Sociālā inženierija Balss klonēšana, dziļviltojumi (angļu val. deepfake), sintētiskas publikācijas, dezinformācija. Krāpnieciski e-pasti, pikšķerēšana Viltus ziņas, clickbait Kiberhuligānisms	4	12	0	0
Kopā:	24	60	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Zināšanas: - Izprot digitālās vides tiesiskos un ētiskos regulējumu nostādnes, sociālās inženierijas metodes, raksturojot skolotāja profesionālo uzvedību tiešsaistes vidē. - Spēj raksturot kiberdrošības pamatprincipus un personas datu aizsardzības mehānismus, iespējamās digitālās vides riskus un draudus.	Pārbaudes veidi: - Patstāvīgais darbs (reālu situāciju analīze), eksāmens (tests). - Grupas projekts, digitālās pēdas analīze, eksāmens (tests). Vērtēšanas kritēriji: - Students spēj identificēt un raksturot tiesiskos un ētiskos regulējumus digitālajā vidē, atpazīst sociālās inženierijas pamatmetodes un teorētiski raksturo skolotāja profesionālās uzvedības un ētikas principus tiešsaistē. - Students pārzina un spēj teorētiski aprakstīt kiberdrošības pamatprincipus un personas datu aizsardzības tehniskos un tiesiskos rīkus, kā arī spēj klasificēt un raksturot digitālās vides riskus un drošības draudus.
Prasmes: - Prot novērtēt tiesiskos un ētiskos riskus, kas saistīti ar informācijas apstrādi, publicēšanu un dalīšanos digitālajā vidē. - Prot identificēt kiberdrošības izaicinājumus izglītības iestādē un izstrādāt atbildīgus risinājumus digitālās vides izmantošanai izglītības kontekstā. - Prot atpazīt un skaidrot sociālās inženierijas uzbrukumus, piemēram, pikšķerēšanu vai viltus ziņas, un rīkoties atbilstoši drošības principiem.	Pārbaudes veidi: - Patstāvīgais darbs (reālu situāciju analīze), digitālās pēdas analīze (pašanalīze). - Grupas projekts, digitālās pēdas analīze (drošības plāns). - Grupas projekts, eksāmens (tests). Vērtēšanas kritēriji: - Students patstāvīgi analizē un kritiski izvērtē reālu situāciju un personīgo publiski pieejamo datu drošību, identificējot un novērtējot riskus, kas rodas, apstrādājot un publicējot informāciju internetā. - Students demonstrē prasmi identificēt specifiskus kiberdrošības izaicinājumus izglītības iestādes vidē, kā arī patstāvīgi izstrādā argumentētu un praktiski pielietojamu personīgās vai profesionālās digitālās drošības plānu. - Students prot praktiski atpazīt sociālās inženierijas uzbrukumus pazīmes, spēj izskaidrot pikšķerēšanas un dezinformācijas izplatīšanas mehānismus un spēj piedāvāt pareizus rīcības soļus drošības incidentu vadībā.

Kompetences: 6. Spēj argumentēti diskutēt par digitālās komunikācijas jautājumiem un kibernetikas jautājumiem, piedāvājot ieteikumus digitālās vides drošības, ētikas un tiesību ievērošanai izglītības jomā. 7. Spēj pieņemt informētus lēmumus par datu aizsardzību un drošības praksēm personīgajā un profesionālajā jomā, kritiski izvērtējot potenciālos riskus digitālajā vidē.	Pārbaudes veidi: 6. Interaktīva spēle, grupas projekts. 7. Digitālās pēdas analīze (pašanalīze un drošības plāns), interaktīva spēle. Vērtēšanas kritēriji: 6. Students spēj argumentēti un strukturēti izskaidrot tiesību un ētikas aspektus digitālajā komunikācijā, kā arī spēj sagatavot, novadīt un pēc tam kritiski analizēt interaktīvu spēli/simulāciju, kurā tiek risinātas kibernetikas un ētikas dilemmas. 7. Students patstāvīgi pieņem un pamato lēmumus par drošu un ētisku rīcību digitālajā vidē, demonstrējot spēju samazināt personas datu apdraudējumus un vadīt riska situācijas personīgajā un profesionālajā darbībā.
--	---

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Patstāvīgais darbs. Reālu situāciju analīze.	20
Grupas projekts	10
Projekts: digitālās pēdas analīze	20
Interaktīva spēle (reāla simulācija)	20
Eksāmens - tests	30
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	3.0	12.0	12.0	0.0		*	