Valsts izglītības
attīstības aģentūra

INOFORMĀCIJAS TEHNOLOĢIJU DROŠĪBA

PROFESIONĀLĀS IZGLĪTĪBAS PROGRAMMAS PARAUGS

Kiberdrošības tehniķis, 4.PKL LKI 4. līmenis

SASKAŅOTS
Izglītības un zinātnes ministrija

2025

Saturs

Profesionālās vidējās izglītības programmas mērķis

Izglītības procesā sagatavot kiberdrošības tehniķi (*junior*), kurš organizācijā atbildīgi veic uzticētos darba pienākumus, kas ietver organizācijas kiberdrošības risinājumu uzturēšanu, reaģēšanu uz kiberdrošības incidentiem un informācijas un komunikāciju tehnoloģiju (turpmāk - IKT) sistēmu drošības testēšanu un ievainojamību ziņojumu apstrādi, nodrošinot datu apstrādi atbilstoši normatīvajiem regulējumiem, nozares prasībām un organizācijas noteiktajai kārtībai.

Profesionālās vidējās izglītības programmas sasniedzamie mācīšanās rezultāti (ietver zināšanas, prasmes un kompetences):

1. iepazīties ar organizācijas IKT vidi un esošo drošības arhitektūru, vadoties pēc organizācijas IKT un IKT drošības aktuālās dokumentācijas (drošības politikas, procedūras, tehniskā dokumentācija).
2. patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības.
3. apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā.
4. novērtēt esošo kiberdrošības prasību izpildi organizācijā.
5. piedāvāt nepieciešamos kiberdrošības uzlabojumus organizācijā.
6. konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos.
7. identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses.
8. veikt kiberdrošības incidentu reģistrēšanu.
9. veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām.
10. patstāvīgi veiktinfo incidentu klasifikāciju atbilstoši organizācijas norādījumiem.
11. veikt kiberdrošības incidentu izpēti sadarbībā ar incidentu izpētē iesaistītajām pusēm.
12. veikt kiberdrošības incidentu informācijas apstrādi.
13. sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta reaģēšanā iesaistītajām pusēm.
14. apkopot informāciju pēc-incidenta ziņojuma sagatavošanai.
15. apkopot incidenta reģistra datus/veiktos pasākumus incidenta reaģēšanas aktivitāšu izvērtēšanai.
16. veidot pēc-incidenta ziņojumus reaģēšanā iesaistītajām pusēm.
17. identificēt potenciālos incidentu reaģēšanas uzlabojumus.
18. novērtēt organizācijas kiberdrošības risinājumus.
19. identificēt iespējamos kiberdrošības risinājumu uzlabojumus.
20. apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.
21. salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus.
22. uzstādīt/ieviest atbilstošākos kiberdrošības risinājumus organizācijas drošības arhitektūrā (infrastruktūra, procesi, dati u.c.) pēc iepriekš noteiktām instrukcijām.
23. nodrošināt ar kiberdrošību saistīto tehnisko risinājumu uzturēšanu atbilstoši organizācijas noteiktajām prasībām un tehniskajai dokumentācijai.

24. ieviest izmaiņas esošajā infrastruktūrā atbilstoši organizācijas kiberdrošības prasībām.
25. sagatavot kiberdrošības risinājumu rezultātu apkopojumu tālākai analīzei.
26. interpretēt no risinājumiem iegūtos rezultātus.
27. iepazīties ar noteiktiem kiberdrošības testu uzdevumiem.
28. apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes.
29. apzināt testa plānu un piemērot drošības testēšanas metodes un rīkus, lai noteiktu iespējamos kiberuzbrukumu vektorus.
30. apgūt testa scenārijus un pēc nepieciešamības pielāgot tos aktuālajai situācijai.
31. precīzi izpildīt testēšanas plānu, scenārijus, izmantojot atbilstošus rīkus un metodes sistēmu ievainojamību identificēšanai.
32. analizēt un dokumentēt testēšanas rezultātus, izstrādāt priekšlikumus organizācijas informācijas sistēmas (turpmāk – IS) kiberdrošības uzlabošanai.
33. sagatavot rekomendācijas identificēto ievainojamību novēršanai, sistēmu un servisu kiberdrošības uzlabošanai.
34. sagatavot un iepazīstināt ar IKT drošības testēšanas rezultātiem tiešo vadītāju, pielietojot profesionālo valodu un terminoloģiju, nodrošinot informācijas skaidru un saprotamu izklāstu.
35. sazināties mutiski un rakstiski valsts valodā, lietojot profesionālo terminoloģiju.
36. sazināties angļu valodā, lietojot profesionālo terminoloģiju.
37. efektīvi komunicēt daudzkultūru vidē.
38. efektīvi iesaistīties komandas darbā.
39. prezentēt informāciju atbilstoši formātam un auditorijai.
40. pielietot IKT rīkus darba uzdevuma veikšanā.
41. ievērot valstī un organizācijā noteiktās kiberdrošības prasības.
42. ievērot tiesību aktu prasības darba aizsardzības un vides aizsardzības jomā.
43. ievērot civilās aizsardzības prasības atbilstoši civilās aizsardzības plāniem un normatīvajiem aktiem.
44. ievērot tiesību aktu prasības elektrodrošības un ugunsdrošības jomā.
45. ievērot un uzraudzīt darba drošības, vides aizsardzības, elektrodrošības, ugunsdrošības, higiēnas un kvalitātes prasības, skaidrojot atsevišķiem darba procesa posmiem atbilstošas prasības.
46. identificēt un izvērtēt riskus, kas var rasties izmantojot IKT.
47. nelaimes gadījumā rīkoties atbilstoši situācijai un sniegt pirmo palīdzību.
48. atbildīgi rīkoties ārkārtas situācijā un izņēmuma stāvokļa laikā, ievērojot valsts noteikto regulējumu un apzinoties savu atbildību nacionālās drošības saglabāšanā.
49. rīkoties atbilstoši organizācijas noteiktajai kārtībai.
50. identificēt, izvērtēt un izmantot profesionālās pilnveides informācijas resursus savas kvalifikācijas celšanai.
51. plānot un pieņemt lēmumus savas profesionālās karjeras veidošanā.
52. izmantot analītisku pieeju profesionālajā darbībā un profesionālās jomas attīstībā.

53. attīstīt un piemērot matemātisko un tehnoloģisko domāšanu ikdienas problēmsituāciju risināšanā.
54. piemērot matemātisko domāšanu, modelējot situācijas un plānojot darba uzdevuma izpildi.
55. aktīvi iesaistīties uzņēmuma darbības attīstībā, piedāvājot jaunas, racionālas idejas darba uzdevuma veikšanai.

Profesionālās izglītības programmas sasniedzamie mācīšanās rezultāti

Profesionālās kvalifikācijas nosaukums	Kiberdrošības tehniķis
LKI līmenis	**LKI 4. līmenis**
Profesionālās kvalifikācijas sasniedzamie mācīšanās rezultāti	• iepazīties ar organizācijas IKT vidi un esošo drošības arhitektūru, vadoties pēc organizācijas IKT un IKT drošības aktuālās dokumentācijas (piemērām kā kiberdrošības politika, procedūras, IKT tehniskā dokumentācija, IT pārvaldības kārtības). • atpazīt autentifikācijas/ autorizācijas tehnoloģijas, datu pārraides tīklu darbības principus, IKT infrastruktūras uzbūvi. • izprast datu pārraides tīklu infrastruktūru un tās komponentes. • patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības. • raksturot datu pārraides tīklu darbības principus, drošības sistēmas, servisu veidus. • skaidrot datu pārraides tīklu uzbūvi, darbību, tīklu drošību. • identificēt, analizēt un apkopot organizācijas kiberdrošības vajadzības, risinājumu drošības vājās vietas, izmantojot kiberincidentu reģistrā pieejamo informāciju. • raksturot kiberdrošības pārvaldības sistēmu, tās komponentes; salīdzināt drošības kontroļu klasifikācijas veidus dažādos standartos; identificēt iesaistītās puses, to atbildības (kiberdrošības pārvaldības lomas) risku novērtēšanas procesos. • izvērtēt sociālās inženierijas metodes un paņēmienus; lietot organizācijas kiberdrošības politiku, procedūras, vadlīnijas, instrukcijas, kā arī obligāto dokumentāciju. • identificēt iespējamos riskus, draudus, ievainojamības, noteikt risku mazināšanas pasākumus. • raksturot iesaistītās puses, to atbildības (kiberdrošības pārvaldības lomas) risku novērtēšanas procesos; informācijas drošības standartus un labo praksi, vispārējās risku pārvaldības principus. • analizēt kiberriska ietekmes un varbūtības kvalitatīvas un kvantitatīvas risku analīzes principus; salīdzināt kiberrisku apstrādes stratēģijas; skaidrot krīzes reaģēšanas soļus. • sagatavot un iepazīstināt ar kiberdrošības risku novērtēšanas rezultātiem, pielietojot profesionālo valodu un terminoloģiju, nodrošinot informācijas skaidru un saprotamu izklāstu. • klasificēt dažādas ar kiberdrošību saistītas vispārīgās teorijas, konceptus, mērķus un prasības, klasifikāciju, specifisko terminoloģiju. • pārbaudīt organizācijas kiberdrošības politiku, procedūras, vadlīnijas, instrukcijas, kā arī obligāto dokumentāciju. • patstāvīgi apzināt, apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā. • analizēt kiberdrošības stratēģiju nacionālā līmenī.

Profesionālās kvalifikācijas nosaukums	Kiberdrošības tehniķis
	• pielietot normatīvo aktu analīzes rīkus, metodes un paņēmienus. • efektīvi komunicēt ar dažādu jomu ekspertiem; apkopot un strukturēt iegūto informāciju par kiberdrošības prasībām. • definēt kiberdrošības profesiju ietvarstruktūras. • salīdzināt informācijas sistēmu drošības standartu nosacījumus (kā piemēram drošības klases, pakalpojumu klasifikāciju, incidentu klasifikācijas principus). • novērtēt esošo kiberdrošības prasību izpildi informācijas sistēmām, risinājumiem, komponentēm. • nosaukt kiberdrošības saistošās likumdošanas un tiesību aktus. • pamatot tehniskās komponentes, kas veido organizācijas IKT resursus (gan piederošos, gan koplietojamos, gan atsevišķi pārvaldāmos). • apzināt atšķirības starp dažādu kiberdrošības profesiju, kiberdrošības lomu, pienākumiem un atbildībām. • skaidrot Latvijas kiberdrošības atbildīgo institūciju hierarhiju un to uzdevumus. • pamatot normatīvo regulējuma prasības un to nozīmi organizācijas kiberdrošības nodrošināšanā. • identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses; veikt kiberdrošības incidentu reģistrēšanu; veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām. • nosaukt incidenta dzīvesciklu (tā sastāvdaļas - priekšizpētei nepieciešamo informāciju). • izskaidrot incidentu apstrādes standartus, labo praksi, digitālās izmeklēšanas nozīmi. • patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem. • izskaidrot incidentu apstrādes rīkus; incidentu klasifikācijas ietvarus, nosacījumus. • novērtēt riskus draudus, ievainojamību klasifikācijas. • patstāvīgi veikt incidentu apstrādi (reģistrēšanu, izpēti, ietekmes novērtēšanu atbilstoši organizācijas norādījumiem). • nosaukt incidenta dzīvescikla posmus. • veikt incidentu obligātās ziņošanas pienākumus, nosacījumus. • patstāvīgi apzināt, apkopot un analizēt organizācijas kiberdrošības inženierijas prasības. • raksturot dažādas ar kiberdrošību saistītas vispārīgās teorijas, konceptus, mērķus un prasības; drošas programmatūras izstrādes dzīvesciklu (SDLC); informācijas sistēmu uzbūvi, komponentes. • pamatot drošas informācijas sistēmas darbības principus, kiberdrošības parametru, mērījumu, veiktspējas rādījumu nozīmi konfigurācijas pārvaldībā. • konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos. • skaidrot drošas programmatūras izstrādes dzīvesciklu (SDLC); informācijas sistēmu uzbūvi, komponentes; drošības arhitektūras principus; konfigurācijas parametru nosacījumus; kriptogrāfijas pamatprincipus.

Profesionālās kvalifikācijas nosaukums	Kiberdrošības tehniķis
	• izmantot drošas informācijas sistēmas darbības principus; pamatot drošības bāzes līnijas (*Security baseline*) pielietojumu; lietot konfigurācijas pārvaldības procedūras; skaidrot autentifikācijas un autorizācijas nozīmi. • sagatavot un novērtēt organizācijas kiberdrošības risinājuma konfigurācijas atbilstību, identificēt iespējamos uzlabojumus. • atpazīt kiberdrošības risinājuma tehniskās prasības; dažādas sociālās inženierijas un krāpniecības metodes; skaidrot kiberhigiēnas pamatprincipus. • veikt informācijas sistēmu stiprināšanas (*hardening*) pasākumus; konfigurācijas failu izveides un analīzes nosacījumus. • iepazīties ar noteiktiem kiberdrošības testu uzdevumiem; apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes. • salīdzināt drošības testēšanas standartus un ietvarus, metodes un rīkus, kas atbalsta prasību apkopošanu un lēmumu pieņemšanas analīzi. • pielietot dažādas drošības testēšanas metodikas (piem. OWASP). • apzināt testa plānu un piemērot drošības testēšanas metodes un rīkus, lai noteiktu iespējamos kiberuzbrukuma vektorus. • paredzēt testēšanas ietekmi uz testējamajām IKT komponentēm; izmantot zināmo ievainojamību avotus (piem. CVE, CERT.LV publicētie u.c.), testēšanas standartus un vadlīnijas. • atšķirt dažādu IS ievainojamības (avotus, vektorus, tipoloģijas). • izstrādāt un veikt sistemātiskus dažāda līmeņa kiberdrošības prasību novērtējumus pēc iepriekš definētiem kritērijiem (izprot atšķirības starp // tai skaitā - *vulnerability scan, penTest, health checks*). • atšķirt objektīva novērtējuma veikšanas paņēmienus, rīkus, matricas; zināmo ievainojamību avotus (piemēram, CVE, CERT.LV publicētie u.c.); izmantot testēšanas standarti un vadlīnijas. • salīdzināt dažādus drošības testēšanas rīkus un risinājumus. • veikt kiberdrošības incidentu izpēti (izmeklēšanu) sadarbībā ar incidentu izpētē iesaistītajām pusēm. • nosaukt incidenta dzīvesciklu (tā sastāvdaļas - priekšizpētei nepieciešamo informāciju), incidenta risināšanā iesaistīto pušu pienākumus un atbildības robežas. • raksturot kiberdrošības uzbrukumu metodes, avotus, vektorus, klasifikāciju. • veikt ar kiberdrošības incidentu saistīto informācijas apstrādi (tai skaitā veikt IS žurnālu (auditācijas pierakstu) analīzi; sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta reaģēšanā, novēršanā iesaistītajām pusēm. • raksturot žurnālu (auditācijas pierakstu) analīzes metodes, paņēmienus, rīkus, struktūru, avotu specifiku, sintakses nosacījumus, analīzes, korelācijas principus. • izprast incidentu apstrādes un incidenta izmeklēšanas procesu atšķirības.

Profesionālās kvalifikācijas nosaukums	Kiberdrošības tehniķis
	• analizēt un apkopot auditācijas pierakstos identificētos notikumus pārskata ziņojumā. • izskaidrot dažādu kiberdrošības atbalsta struktūru (SOC, CERT, HelpDesk) darbības pamatprincipus, galvenās atšķirības, atbilstības prasības. • novērtēt digitālās izmeklēšanas atvērto rīku (OSINT u.c.) darbības ierobežojumus. • apkopot un analizēt organizācijas kiberdrošības risinājumu tehniskos kritērijus, rezultatīvos rādītājus, veiktspējas metrikas; identificēt iespējamos kiberdrošības risinājumu uzlabojumus. • skaidrot drošības sistēmu veidus, datu pārraides tīklu infrastruktūru un tās komponentes, drošas programmatūras izstrādes dzīvesciklu. • pamatot kiberdrošības parametru, mērījumu, veiktspējas rādītāju nozīmi konfigurācijas pārvaldībā. • apzināt, atlasīt, grupēt dažāda veida un līmeņa tehniskās prasības (kā piemēram, kiberdrošības, funkcionālās/nefunkcionālās) prasības nepieciešamajam IKT risinājumam. • raksturot drošības arhitektūras principus, prasību ieviešanas procedūras, konfigurācijas parametru nosacījumus. • skaidrot gala ierīču (angl. *end-point*) drošības nozīmi kopējā drošības arhitektūrā. • salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus. • izvērtēt sistēmu integrācijas metodes, savietojamības prasības, drošības bāzes līnijas (angl. *Security baseline*). • pamatot izmaiņu pārvaldības ietekmi uz darbības nepārtrauktības nodrošināšanu. • ieviest un uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām. • aprakstīt izmaiņu pārvaldības principus, testēšanas veidus, metodes, rīkus. • apzināt datu aizsardzības, kiberdrošības, izmaiņu pārvaldības risinājumus. • salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus (OT). • skaidrot drošības sistēmu veidus, datu pārraides tīklu infrastruktūru un tās komponentes. • pamatot izmaiņu pārvaldības ietekmi uz darbības nepārtrauktības nodrošināšanu. • uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām. • raksturot drošības arhitektūras principus, to sastāvdaļas. • aprakstīt drošības metrikas un to nozīmi. • apkopot nepieciešamo informāciju, kas saistīta ar iekšējās izmeklēšanas darbībām, piemērot atbilstošus incidentu izmeklēšanai nepieciešamos aizsardzības pasākumus. • skaidrot izmeklēšanas darbību secību, pierādījumu apstrādes kārtību, salīdzināt digitālās izmeklēšanas metodes un rīkus, aprakstīt digitālo pierādījumu saglabāšanas principus, incidentu apstrādes dzīvesciklu, pierādījumu apstrādes dzīvesciklu. • pamatot dokumentācijas un būtisko atribūtu nozīmi incidentu izmeklēšanas un pierādījumu vākšanas procesā, pielietot digitālo pierādījumu apstrādes standartus, skaidrot digitālo artefaktu apstrādes rīku darbības principus.

Profesionālās kvalifikācijas nosaukums	Kiberdrošības tehniķis
	• sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta izmeklēšanā iesaistītajām pusēm, identificēt, apkopot un saglabāt digitālos pierādījumus, nodrošinot pierādījumu nemainīgumu (integritāti). • nosaukt izmeklēšanas darbību secību, pierādījumu apstrādes kārtību, digitālās izmeklēšanas metodes un rīkus, digitālo pierādījumu saglabāšanas principus, incidentu apstrādes dzīvesciklu, pierādījumu apstrādes dzīvesciklu. • skaidrot dokumentācijas un būtisko atribūtu nozīmi incidentu izmeklēšanas un pierādījumu vākšanas procesā, digitālo pierādījumu apstrādes standartus, digitālo artefaktu apstrādes rīku darbības principus.

Profesionālās izglītības programmas īstenošanai obligātie vispārējās vidējās izglītības mācību priekšmetu pamatkursi un padziļinātie kursi

1.Programmas pamata daļa:

- Latviešu valoda I un Literatūra I (optimālais līmenis)
- Matemātika (optimālais līmenis)
- Svešvaloda I (B2) (optimālais līmenis)
- Sports (vispārīgais līmenis)
- Valsts aizsardzības mācība
- Sabiedrības un cilvēka drošība (1., 2.līmenis)

2.Programmas mainīgā daļa:

- Sociālās zinības un vēsture (vispārīgais līmenis)
- Svešvaloda (B1) (vispārīgais līmenis)
- Dabaszinības (vispārīgais līmenis)
- Fizika I (optimālais līmenis)
- Matemātika II (augstākais līmenis)
- Svešvaloda II (CI) (augstākais līmenis)
- Fizika II (augstākais līmenis)

Profesionālās izglītības apguves iespējas

Profesionālās izglītības programmas veids (turpmāk – programma)		Profesionālās vidējās izglītības programma		Profesionālās tālākizglītības programma
Kiberdrošības tehniķis	Prasības attiecībā uz iepriekš iegūto izglītību	**Pamatizglītība**	**Vidējā izglītība**	**Profesionālā vidējā izglītība IT jomā**
	Programmas īstenošanas ilgums gados	**4 gadi**	**1,5 gads**	**-**
	Programmas īstenošanas ilgums stundās	**5736 stundas**	**2120 stundas**	**960 stundas**
	LKI līmenis	**LKI 4. līmenis**		**LKI 4. līmenis**
	Izglītības klasifikācijas kods	**33 483 02 1**	**35b 483 02 1**	**30T 483 02 1**

Profesionālās izglītības programmas īstenošanas plānojums

LKI līmenis/ Kvalifikācijas nosaukums/ Izglītības dokuments	Kurss (ja attiecināms)	Profesionālo kompetenču moduļi		Mūžizglītības kompetenču moduļi (līmenis)	Vispārējās vidējās izglītības mācību priekšmetu pamatkursi un padziļinātie kursi (ja attiecināmi)
		Nosaukums	Noslēguma pārbaudījums		Nosaukums (apguves līmenis)
LKI 4. līmenis /Kiberdrošības tehniķis	1. kurss	IKT un drošības arhitektūras pamati Kiberdrošības un risku pārvaldības pamati IKT un kiberdrošības normatīvo aktu piemērošana Incidentu klasifikācija, reaģēšana, analīze, novēršana	NP	Sabiedrības un cilvēka drošība (1.līmenis) Informācijas un komunikācijas tehnoloģijas (1., 2.līmenis)	Latviešu valoda I un Literatūra I (optimālais) (NP-3. kursā) Matemātika I (optimālais) (NP-3. kursā) Svešvaloda I (B2) (NP-3. kursā) Sports (vispārīgais) Sociālās zinības un vēsture (vispārīgais) Svešvaloda (B1) Fizika I (optimālais) Valsts aizsardzības mācība
	2. kurss	IKT un drošības arhitektūras pamati Kiberdrošības un risku pārvaldības pamati Incidentu klasifikācija, reaģēšana, analīze, novēršana IS drošības inženierija, IS stiprināšana, konfigurācijas uzturēšana IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana 1	NP NP	Valodas, kultūras izpratne un izpausmes (1.līmenis) Iniciatīva un uzņēmējdarbība (1.līmenis)	
	3. kurss	IS drošības inženierija, IS stiprināšana, konfigurācijas uzturēšana IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana 1 Kiberdrošības incidentu izmeklēšana 1 Kiberdrošības risinājumu (uzstādīšana, uzturēšana, novērtēšana) 1	NP	Sabiedrības un cilvēka drošība (2.līmenis) Valodas, kultūras izpratne un izpausmes (2.līmenis) Iniciatīva un uzņēmējdarbība (2.līmenis)	
	4. kurss	IS drošības inženierija, IS stiprināšana, konfigurācijas uzturēšana IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana 1 Kiberdrošības incidentu izmeklēšana 1 Kiberdrošības risinājumu (uzstādīšana, uzturēšana, novērtēšana) 1	NP		Matemātika II (augstākais) Fizika II (augstākais) Svešvaloda II (augstākais)

*NP – noslēguma pārbaudījums

Modulārās profesionālās izglītības programmas parauga moduļu karte

C		**Kiberdrošības incidentu izmeklēšana 2 PC 5%**	**Kiberdrošības risinājumu (uzstādīšana, uzturēšana, novērtēšana) 2 PC 5%**	**Radio sakaru pamati PC 5%**	**Mākslīgais intelekts PC 5%**
B	**Iniciatīva un uzņēmējdarbība (1. un 2. līmenis)**				
	Valodas, kultūras izpratne un izpausmes (1. un 2. līmenis)	**Kiberdrošības incidentu izmeklēšana 1 PB5 10%**	**Kiberdrošības risinājumu (uzstādīšana, uzturēšana, novērtēšana) 1 PB6 12%**	**Kiberdrošības tehniķa prakse PB7**	
	Informācijas un komunikācijas tehnoloģijas (1. un 2. līmenis)	**IKT un kiberdrošības normatīvo aktu piemērošana PB1 8%**	**Incidentu klasifikācija, reaģēšana, analīze, novēršana PB2 12%**	**IS drošības inženierija, IS stiprināšana, konfigurācijas uzturēšana PB3 12%**	**IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana 1 PB4 13%**
A	**Sabiedrības un cilvēka drošība (1. un 2. līmenis)**	**IKT un drošības arhitektūras pamati PA1 13%**	**Kiberdrošības un risku pārvaldības pamati PA2 10%**		

Kiberdrošības tehniķis (LKI 4. līmenis)

MODUĻA IKT un drošības arhitektūras pamati APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmes organizācijas IKT vides un drošības arhitektūras veidošanā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. iepazīties ar organizācijas IKT vidi un esošo drošības arhitektūru, vadoties pēc organizācijas IKT un IKT drošības aktuālās dokumentācijas (piemērām kā kiberdrošības politika, procedūras, IKT tehniskā dokumentācija, IT pārvaldības kārtības). 2. patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem. 3. patstāvīgi veikt incidentu apstrādi (reģistrēšanu, izpēti, ietekmes novērtēšanu atbilstoši organizācijas norādījumiem).
Moduļa ieejas nosacījumi	Iegūta pamatizglītība.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie kārto moduļa noslēguma pārbaudes darbu, kurā ir teorētisko zināšanu pārbaudes jautājumi un praktiskais uzdevums – izveidot IKT drošības arhitektūru dotā scenārijā, vadoties pēc aktuālas drošība sdokumentācijas.
Moduļa nozīme un vieta kartē	Modulis " IKT un drošības arhitektūras pamati " ir A daļas modulis. To apgūst vienlaicīgi ar moduli "Kiberdrošības risku un pārvaldības pamati", kā arī B daļas moduļiem " IKT un kiberdrošības normatīvo aktu piemērošana " un " Incidentu klasifikācija, reaģēšana, analīze, novēršana ".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA IKT un drošības arhitektūras pamati SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.**Spēj:** iepazīties ar organizācijas IKT vidi un esošo drošības arhitektūru, vadoties pēc organizācijas IKT un IKT drošības aktuālās dokumentācijas (piemērām kā kiberdrošības politika, procedūras, IKT tehniskā dokumentācija, IT pārvaldības kārtības). **Zina:** autentifikācija/ autorizācijas tehnoloģijas, datu pārraides tīklu darbības principi, IKT infrastruktūras uzbūve.	1.1.IS uzbūve un tās komponentes. 5 % no moduļa kopējā apjoma	1.1.1. IS funkcionalitāte un loma organizācijas darbības nodrošināšanā.	Saprot IS nozīmi organizācijas darbībā	Apraksta dažādu IS veidu pielietojumu dažādās organizācijās	Pielāgo un iesaka efektīvus IS risinājumus konkrētai organizācijai
		1.1.2. IS komponentes un to loma IS darbībā.	Nosauc IS komponentes un izskaidro to galvenās funkcijas.	Izskaidro IS komponenšu savstarpējo mijiedarbību un nozīmi IS darbībā.	Analizē un plāno IS uzbūvi, ņemot vērā organizācijas vajadzības un drošības prasības.
	1.2.IKT pamati. 40 % no moduļa kopējā apjoma	1.2.1.Datoru arhitektūras pamati.	Nosauc datorsistēmas pamata komponentes un to funkciju.	Analizē un salīdzina dažādu komponenšu darbību un to veiktstpēju.	Izvēlas komponentes un konfigurē datorsistēmu balstoties uz veiktspējas prasībām.
		1.2.2.OS pamati.	Izmanto Windows un Linux OS ikdienas darbībām.	Instalēt un konfigurēt OS, veic diagnostiku un atkļūdošanu.	Administrē OS, optimizē to darbību, pielāgo konfigurāciju atbilstoši dažādām situācijām.
		1.2.3.Programmēšanas pamati un algoritmi.	Saprot programmēšanas pamatprincipus, datu tipus un vadības struktūras.	Veido vienkāršus algoritmus un programmē mazus skriptus kādā programmēšanas valodā.	Izstrādā un optimizē algoritmus, pielieto efektīvas datu struktūras un analizē programmu veiktspēju.
		1.2.4.Datu pārraides tīklu pamati.	Saprot tīkla pamatprincipus un nosauc tīkla komponentes.	Konfigurē nu testē lokālus datu pārraides tīklus, veic kļūdu diagnostiku un novēršanu.	Veido uz uztur tīkla infrastruktūru, ievieš drošības risinājumus

Izprot: datu pārraides tīklu infrastruktūra un tās komponentes.					un optimizē to veiktspēju.
		1.2.5.Mākoņdatošanas pamati.	Saprot mākoņdatošanas jēdzienu un nosauc populārākos pakalpojumu sniedzējus.	Konfigurē un izmanto mākoņpakalpojumus.	Plāno un optimizē mākoņrisinājumus, nodrošina to drošību un efektivitāti.
		1.2.6.Ievads IKT arhitektūras modeļos.	Nosauc dažādus IKT arhitektūras modeļus (SABSA, COBIT, TOGAF) un saprot to lomu IKT sistēmu pārvaldībā un drošībā.	Identificē modeļu elementus organizācijas IKT dokumentācijā un procedūrās (piemēram, drošības vadlīnijās, IT pārvaldības procesos, arhitektūras dokumentācijā).	Praktiski pielieto konkrētus SABSA, COBIT vai TOGAF principus savā darbā, piemēram, palīdzot nodrošināt IT pārvaldības atbilstību (COBIT), drošības politiku ievērošanu (SABSA) vai arhitektūras dokumentācijas uzturēšanu (TOGAF).
	1.3.Autentifikācijas tehnoloģijas. 15 % no moduļa kopējā apjoma	1.3.1. Autentifikācijas metodes.	Nosauc un saprot dažādas autentifikācijas metodes.	Atpazīst un pielieto autentifikācijas metodes organizācijas IKT sistēmās.	Konfigurē un uztur autentifikācijas risinājumus, nodrošinot to atbilstību drošības vadlīnijām.
		1.3.2. Daudzfaktoru autentifikācija.	Saprot daudzfaktoru autentifikācijas jēdzienu un tās lomu.	Ievieš un konfigurē daudzfaktoru autentifikācijas risinājumus.	Administrē MFA sistēmas un risina ar tām saistītās problēmsituācijas.
		1.3.3. Kriptogrāfijas loma un metodes autentifikācijā.	Saprot kriptogrāfijas lomu autentifikācijas procesos, nosauc piemērus.	Izmanto kriptogrāfijas rīkus (OpenSSL, GPG) vienkāršām autentifikācijas darbībām.	Konfigurē un izmanto kriptogrāfiskās autentifikācijas metodes, piemēram, digitālos sertifikātus, SSH atslēgas, drošus paroļu uzglabāšanas mehānismus.
2.**Spēj:** patstāvīgi apzināt un apkopot	2.1. IKT resursu uzskaites rīki.	2.1.1.IKT resursu pārvaldība.	Saprot IKT resursu pārvaldības	Veic IKT resursu inventarizāciju un uztur uzskaites sistēmu,	Patstāvīgi uztur IKT resursu uzskaiti, analizē datus un

organizācijas kiberdrošības prasības. **Zina**: datu pārraides tīklu darbības principi, drošības sistēmu, servisu veidi. **Izprot:** datu pārraides tīklu uzbūve, darbība, tīklu drošība.	10 % no moduļa kopējā apjoma.		pamatprincipus un to nozīmi organizācijā.	ievērojot organizācijas prasības. Strādā ar resursu pārvaldības dokumentāciju un palīdz veikt auditus.	atklāj neatbilstības. Pielāgo resursu pārvaldības procedūras, ievērojot organizācijas politikas un drošības prasības.
		2.1.2.Uzskaites un monitoringa rīki(GLPI, OCS Inventory, MS SCCM un tml.).	Nosauc populārākos resursu uzskaites un monitoringa rīkus.	Meklēt informāciju par IT resursiem, pievieno un rediģē ierakstus. Analizē uzskaites rīku datus.	Veic pamata konfigurācijas uzskaites un monitoringa rīkos, piemēram, pievienot jaunus resursus vai veic ierakstu sinhronizāciju.
	2.2. Informācijas drošības standarti un ietvari. 15 % no moduļa kopējā apjoma.	2.2.1. Informācijas drošības pamatprincipi(CIA).	Saprot CIA principus un to nozīmi IKT drošībā.	Identificē drošības riskus, kas CIA principus apdraud.	Piedalās drošības risku novēršanas pasākumos. Piemēro CIA principus organizācijas drošības politikās/procedūrās.
		2.2.2.Starptautiskie drošības standarti.(ISO, CIS un tml.).	Zina drošības standartus un saprot to nozīmi IKT drošībā.	Identificē organizācijā izmantos standartus un seko to vadlīnijām ikdienas darbībās.	Palīdz nodrošināt sistēmu atbilstību drošības standartiem, sagatavot dokumentāciju un/vai piedalīties auditā.
		2.2.3. IT pārvaldības ietvari(COBIT, ITIL un tml.).	Zina pārvaldības ietvaru pamatprincipus un saprot to lomu.	Identificē kā konkrēti ietvari tiek izmantoti organizācijas IKT procesos.	Palīdz uzturēt ietvaru prasībām atbilstošu dokumentāciju un procesus.
		2.2.4. Datu aizsardzības regulējumi(GDPR, eIDAS un tml.).	Zina vispārīgus datu aizsardzības regulējumus un to nozīmi.	Identificē situācijas, kurās ir attiecināmas konkrēti datu aizsardzības regulējumi. Ievēro datu aizsardzības prasības.	Palīdz nodrošināt atbilstību datu aizsardzības regulām, piemēram, veicot dokumentācijas uzturēšanu.
	2.3. Pieejas kontrole un lietotāju tiesību pārvaldība.	2.3.1.Piekļuves kontroles pamatprincipi	Saprot piekļuves kontroles pamatprincipus (RBAC, *least privilege*)	Identificē un pārbaude lietotāju piekļuves tiesības sistēmās.	Pārvalda piekļuves kontroles mehānismus un uztur

	15 % no moduļa kopējā apjoma				lietotāju tiesību auditus.
		2.3.2. Lietotāju kontu pārvaldība un lomas.	Saprot lietotāju kontu un lomu koncepciju (lokālie konti, AD).	Uztur un pārvalda lietotāju kontus un to piekļuves tiesības organizācijas IT vidē.	Pārvalda lietotāju piekļuves tiesības sistēmās, veic kontu auditus un nodrošina atbilstību organizācijas drošības politikai.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited
4. "Practical Cybersecurity Architecture", Ed Moyle, Diana Kelley, Packt Publishing, 2023., 418.lpp
5. "Security Engineering: A Guide to Building Dependable Distributed Systems", Ross J. Anderson, Wiley, 2020., 1232.lpp
6. "Building Secure and Reliable Systems: Best Practices for Designing, Implementing and Maintaining Systems", Heather Adkins, Betsy Beyer, Paul Blankinship, et al., O'Reilly Media, 2020., 555.lpp
7. "CompTIA Security+ Guide to Network Security Fundamentals (MindTap Course List", Mark Ciampa, Cengage Learning, 2024., 608.lpp
8. "Principles of Information Security (MindTap Corse List)", Michael Whitman, Herbert Mattord, Cengage Learning, 2021., 752.lpp
9. Networking basics: The complete guide on network protocols and OSI model. Includes a useful section about wireless home networking. - USA: Giale Ltd, 2020. 120 lpp
10. Helmke, Matthew. Ubuntu Linux: Unleashed / Matthew Helmke. - 14th edition. - London: Pearson Education, 2021. - 714 lpp
11. Haber, Morey. Privileged attack vectors: Building effective cyber-defense strategies to protect organizations / Morey Haber. - Second edition. - Berkley: APress, 2020. – 419 lpp
12. Steinberg, Joseph. Cybersecurity for dummies: the latest developments in cybersecurity / Joseph Steinberg. - 2nd edition. - New York: John Wiley & Sons Inc, 2022. - 416 lpp

MODUĻA Kiberdrošības un risku pārvaldības pamati APRAKSTS

Moduļa mērķis	Attīstīt izglītojamo spējas veikt kiberrisku novērtējumus, sniegt informāciju par rezultātu ieinteresētajām pusēm.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. identificēt, analizēt un apkopot organizācijas kiberdrošības vajadzības, risinājumu drošības vājās vietas, izmantojot kiberincidentu reģistrā pieejamo informāciju. 2. identificēt iespējamos riskus, draudus, ievainojamības, noteikt risku mazināšanas pasākumus.
Moduļa ieejas nosacījumi	Iegūta pamatizglītība.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie izstrādā, novada un prezentē divus dažādus kiberriska novērtējuma rezultātus (informācijas sistēmas komponentēm).
Moduļa nozīme un vieta kartē	Modulis "Kiberdrošības un risku pārvaldības pamati" ir A daļas modulis, ko izglītojamie apgūst vienlaicīgi ar "IKT un drošības arhitektūras pamati" moduli, B daļas moduļiem " IKT un kiberdrošības normatīvo aktu piemērošana " un " Incidentu klasifikācija, reaģēšana, analīze, novēršana ".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Kiberdrošības un risku pārvaldības pamati SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.**Spēj:** identificēt, analizēt un apkopot organizācijas kiberdrošības vajadzības, risinājumu drošības vājās vietas, izmantojot kiberincidentu reģistrā pieejamo informāciju. **Zina:** kiberdrošības prāvaldības sistēma, tās komponentes. Drošības kontroļu klasifikācijas veidius dažādos standartos; Iesaistītās puses, to atbildības (kiberdrošības pārvaldības lomas) risku novērtēšanas procesos **Izprot:** sociālās inženierijas metodes un paņēmieni; organizācijas kiberdrošības politika, procedūra, vadlīnijas, instrukcijas, kā arī obligato dokumentāciju.	20% no moduļa kopējā apjoma	1.1.Informācijs drošības jēdzieni, prasības, koncepti un kontroles dāžados standartos (ISO 27001, NIST, OWASP) .	Raksturo un klasificētdažus no drošības jēdzieniem, konceptiem, prasībām un kontrolēm.	Strukturēti raksturo un klasificē drošības jēdzienus, konceptus, prasības un drošības kontroles.	Strukturēti raksturo, klasificē un izskaidro priekšrocības un trūkumus dažādu drošības jēdzienu, konceptu, prasību un drošības kontrlļu pielietojumam.
	20% no moduļa kopējā apjoma	1.2.Kiberdrošības pārvaldības sistēma (ISO 27001) un atbildību sadalījums risku pārvaldībā	Vispārīgi uzskaita iesaistītās puses un to atbildības, nesniedzot piemērus un skaidrojumus.	Precīzi raksturo iesaistītās puses kiberdrošības pārvaldībā, sasaistot to lomas ar konkrētiem procesiem un organizācijas struktūru.	Analizē un iesaka optimālu iesaistīto pušu sadarbības modeli, definējot to lomas un atbildības reālās kiberdrošības pārvaldības situācijās.
2.**Spēj:** identificēt iespējamos riskus, draudus, ievainojamības,	15% no moduļa kopējā apjoma	2.1.Kiberdrošības risku analīzes process	Identificē tikai vispārīgus kiberdrošības izaicinājumus, analizējot vēsturiski pieejamo	Veic pamatotu analīzi, identificē būtiskās drošības vājās vietas un sasaista tās ar	Sistemātiski analizē incidentu reģistra datus, identificējot gan specifiskas vājās

noteikt risku mazināšanas pasākumus. **Zina:** iesaistītās puses, to atbildības (kiberdrošības pārvaldības lomas) risku novērtēšanas procesos; Informācijas drošības standarti un labā prakse, vispārējās risku pārvaldības principi **Izprot:** kiberriska ietekmes un varbūtības kvalitatīvas un kvantitatīvas risku analīzes principus. Kiberrisku apstrādes stratēģijas. Krīzes reaģēšanas soļi.			informāciju par kiberincidentiem	organizācijas kiberdrošības vajadzībām.	vietas, gan stratēģiskas vajadzības, piedāvājot konkrētus risinājumus.
	15% no moduļa kopējā apjoma	2.2. Kiberdrošības risku mazināšanas pasākumu plāns	Identificē vispārīgus draudus un riskus, piedāvā minimālus mazināšanas pasākumus bez detalizēta pamatojuma.	Identificē būtiskus draudus un ievainojamības, piedāvājot loģiskus un pamatotus risku mazināšanas pasākumus.	Precīzi identificē daudzveidīgus draudus un ievainojamības, sasaistot tos ar uzņēmuma darbību, un izstrādā risku mazināšanas plānu
3.**Spēj:** sagatavot un iepazīstināt ar kiberdrošības risku novērtēšanas rezultātiem, pielietojot profesionālo valodu un terminoloģiju, nodrošinot informācijas skaidru un saprotamu izklāstu. **Zina:** dažādas ar kiberdrošību saistītas vispārīgās teorijas, koncepti, mērķi un prasības. klasifikācija, specifiskā terminoloģija. **Izprot:** organizācijas kiberdrošības politika, procedūra, vadlīnijas,	15% no moduļa kopējā apjoma	3.1. Kiberrisku novērtējuma, plāna komunikācija iesaisītajām pusēm	Prezentē rezultātus ar vispārīgu terminoloģiju un neskaidru informācijas struktūru, radot grūtības saprast būtiskos aspektus.	Strukturēti un skaidri prezentē risku novērtēšanas rezultātus, izmantojot profesionālo terminoloģiju, lai auditorija saprastu būtiskākos aspektus.	Veiksmīgi pielāgo informācijas izklāstu auditorijai, skaidri un pārliecinoši iepazīstina ar risku novērtējuma mētrikām, izmantojot profesionālu valodu un vizualizācijas.
	15% no moduļa kopējā apjoma	3.2. Sociālā eksperimenta (pikšķerēšanas testa novērtējuma) rezultātu prezentācija	Prezentē rezultātus ar vispārīgu terminoloģiju un neskaidru informācijas struktūru, radot grūtības saprast būtiskos aspektus.	Strukturēti un skaidri prezentē risku novērtēšanas rezultātus, izmantojot profesionālo terminoloģiju, lai auditorija saprastu būtiskākos aspektus.	Veiksmīgi pielāgo informācijas izklāstu auditorijai, skaidri un pārliecinoši iepazīstina ar risku novērtējuma mētrikām, izmantojot profesionālu valodu un vizualizācijas.

instrukcijas, kā arī obligāto dokumentāciju.					

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA IKT un kiberdrošības normatīvo aktu piemērošana APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmes IKT un kiberdrošības normatīvo aktu piemērošanai organizācijā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.patstāvīgi apzināt, apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā. 2. novērtēt esošo kiberdrošības prasību izpildi informācijas sistēmām, risinājumiem, komponentēm. 3. apzināt atšķirības starp dažādu kiberdrošības profesiju, kiberdrošības lomu, pienākumiem un atbildībām. 4. efektīvi komunicēt ar dažādu jomu ekspertiem. Apkopot un strukturēt iegūto informāciju par kiberdrošības prasībām.
Moduļa ieejas nosacījumi	Apgūti A daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudījumu, kurā ir teorētisko zināšanu pārbaudes jautājumi un praktiskā darba daļa - dotās situācijas analīze atbilstoši normatīvajiem aktiem.
Moduļa nozīme un vieta kartē	Modulis " IKT un kiberdrošības normatīvo aktu piemērošana " ir B daļas modulis. To apgūst vienlaicīgi ar A daļas moduļiem "IKT un drošības arhitektūras pamati", "Kiberdrošības un risku pārvaldības pamati" un " Incidentu klasifikācija, reaģēšana, analīze, novēršana ".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA IKT un kiberdrošības normatīvo aktu piemērošana SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis*
1.**Spēj:** patstāvīgi apzināt, apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā. **Zina:** izprot kiberdrošības stratēģiju nacionālā līmenī. **Izprot:** Normatīvo aktu analīzes rīki, metodes un paņēmienus.	1.1.Normatīvo aktu analīzes pamatprincipi 25% no moduļa kopējā apjoma	1.1.1. Normatīvo aktu hierarhija un struktūras izpratne. 1.1.2. Normatīvo aktu piemērojamības novērtēšana.	Apraksta galvenos normatīvo aktu veidus un to hierarhiju. Apraksta normatīvo aktu struktūras pamatprincipus. Apraksta galvenās situācijas, kurās nepieciešama normatīvo aktu piemērojamības novērtēšana. Sameklē vienkāršus piemērus normatīvo aktu prasību ievērošanai organizācijā.	Izskaidro normatīvo aktu hierarhijas un to lomu organizācijas kiberdrošības politikas veidošanā. Izskaidro dažādu līmeņu normatīvo aktu mijiedarbību organizācijas drošības prasību īstenošanā. Apspriež normatīvo aktu piemērošanu specifiskām organizācijas vajadzībām. Izskaidro normatīvo aktu prasības organizācijas procesos.	Analizē normatīvo aktu hierarhijas nozīmi organizācijas kiberdrošības jautājumos. Analizē normatīvo aktu integrāciju organizācijas drošības stratēģijā. Analizē normatīvo aktu ietekmi organizācijas drošības politikā. Analizē normatīvo aktu piemērošanu organizācijā.

	1.2. Normatīvo aktu analīzes rīki, metodes un paņēmieni	1.2.1. Automatizētie rīki (piem. riski.lv u.c.) 1.2.2. Manuāla analīze. 1.2.3. Konteksta interpretācija un tās nozīme. 1.2.4. Praktiskie uzdevumi un scenāriji normatīvo aktu analīzē.	Apraksta galvenos automatizētos analīzes rīkus, manuālās analīzes pamatprincipus, konteksta interpretācijas nozīmi kiberdrošības prasību analīzē. Apraksta automatizēto rīku un manuālās analīzes pieeju izmantošanu, identificē situācijas, kurās ir būtiska konteksta interpretācija. Parādīt rīku izmantošanu vienkāršas analīzes veikšanā, vadoties pēc norādījumiem.	Salīdzina automatizēto un manuālo analīzes rīku efektivitāti dažādās situācijās., izskaidro konteksta interpretācijas nozīmi. Apspriež piemērotākā analīzes rīka vai metodes izvēli konkrētam uzdevumam. Izskaidro kā konteksta interpretācija uzlabo normatīvo aktu piemērošanu organizācijā. Izskaidro rīku izmantošanu vienkāršas analīzes veikšanā.	Analizē dažādu rīku un paņēmienu savstarpējo mijiedarbību normatīvo aktu analīzē, analizē konteksta interpretācijas stratēģisko nozīmi normatīvo prasību risināšanā. Analizē dažādus analīzes rīku un metožu piemērošanu konkrētām situācijām. Analizē konteksta interpretāciju risinājumu piedāvājumam normatīvo aktu prasībām. Patstāvīgi pielieto rīkus un metodes normatīvo aktu analīzē.
	1.3. Nacionālās kiberdrošības stratēģijas pārskats	1.3.1. Stratēģijas vīzija, prioritātes un mērķi 1.3.2.Atbildīgās iestādes/ organizācijas un to loma kiberdrošības stratēģijas prioritāšu, rīcības virzienu noteikšanā un stratēģijas ieviešanā.	Apraksta nacionālās kiberdrošības stratēģijas pamatstruktūru un galvenos elementus. Uzskaita nacionālās kiberdrošības stratēģijas prioritātes un rīcības virzienus. Apraksta atbildīgās organizācijas, kas iesaistītas stratēģijas ieviešanā. Apraksta sadarbības starp valsts un	Izskaidro nacionālās kiberdrošības stratēģijas prioritātes, mērķus, un to nozīmi valsts drošības stiprināšanā. Izskaidro stratēģijas uzdevumus un to izpildes mehānismus. Izskaidro organizāciju, kas iesaistītas stratēģijas ieviešanā galvenās funkcijas un pienākumus. Apspriež atbildīgo organizāciju sadarbību	Analizē kiberdrošības stratēģijas mērķu un uzdevumu ietekmi uz organizācijas darbību. Izskaidro organizāciju lomu stratēģijas ieviešanā un prioritāšu noteikšanā. Sagatavo pārskatu par stratēģijas uzdevumu izpildes ietekmi uz organizācijas

			privātajām institūcijām nepieciešamību. Sagatavo vienkāršu pārskatu par stratēģijas rīcības virzieniem, mērķiem un iesaistīto iestāžu lomu.	stratēģijas ieviešanas procesā. Izskaidro nacionālās kiberdrošības stratēģijas uzdevumu izpildes ietekmi uz organizācijas darbību.	kiberdrošības stratēģiju. Argumentēti prezentē analīzes rezultātusun ieteikumus.
	1.4. Starptautiskās sadarbības nozīme kiberdrošībā	1.4.1. Eiropas Savienības iniciatīvas un projekti kiberdrošības stiprināšanai. 1.4.2. Starpautiskie IKT un kiberdrošības standarti	Uzskaita galvenās ES kiberdrošības iniciatīvu un globālo kiberdrošības standartu mērķus un nozīmi. Apraksta kā ES iniciatīvas un globālie standarti palīdz kiberdrošības stiprināšanā un starptautiskās sadarbības veicināšanā. Parāda vienkāršus piemērus standartu izmantošanai organizācija'.	Izskaidro ES kiberdrošības projektu un iniciatīvu elementus un to ietekmi uz dalībvalstīm un starptautisko standartu piemērošanu kiberdrošības politikās un tehnoloģiskajos risinājumos. Izprot ES projektu ietekmi un sadarbības nepieciešamību kiberdrošības jomā. Izskaidro kā starptautiskie standarti veicina vienotu pieeju risku pārvaldībai un drošības prasībām. Analizē ES kiberdrošības projektu pielietojumu organizācijā.	Analizē ES kiberdrošības iniciatīvu efektivitāti un pielietokjumu organizācijā. Izvērtē starptautisko standartu nozīmi integrācijai organizācijā. Formulē stratēģiskos drošības mērķus organizācijā, izmantojot starptautiskos standartus un iniciatīvas. Izvērtē starptautiskos standartus konkrētu drošības izaicinājumu risināšanā. Analizē starptautiskās sadarbības un standartu integrācijas ietekmi organizācijas kiberdrošības spēju uzlabošanā.
2.Spēj: efektīvi komunicēt ar dažādu jomu ekspertiem. Apkopot un strukturēt	2.1. Informācijas sistēmu drošības standartu pārskats.	2.1.1. Kontroles un labās prakses piemēri (NIST).	Apraksta NIST kontroles pamatprincipus un vispārējos labās prakses piemērus.	Izskaidro NIST kontroles un labās prakses piemēru piemērošanas nozīmīgumu.	Analizē informācijas drošības vadības sistēmu un kontroles piemērošanas ietekmi

iegūto informāciju par kiberdrošības prasībām. **Zina:** kiberdrošības profesiju ietvarstruktūras. **Izprot:** informācijas sistēmu drošības standartu nosacījumus (kā piemēram drošības klases, pakalpojumu klasifikāciju, incidentu klasifikācijas principus).	25% no moduļa kopējā apjoma	2.1.2.Pakalpojumu pārvaldības piemēri (ITIL).	Apraksta ITIL pamatprincipus pakalpojumu pārvaldībā. Apraksta, kā NIST kontroles un labās prakses piemēri palīdz mazināt kiberdrošības riskus. Novērtē ITIL principu lomu drošības pārvaldības procesā.	Izskaidro ITIL pieeju pakalpojumu pārvaldībai un tās saistību ar drošību. Izskaidro NIST kontroles mehānismu savstarpējo papildināmību drošības pārvaldībā. Izskaidro ITIL pieejas pielietojumu drošības un pakalpojumu kvalitātes uzlabošanā.	uz organizācijas drošības stratēģiju. Novērtē ITIL un NIST piemēru efektivitāti organizācijas drošības un pakalpojumu pārvaldības pilnveidošanā. Veic, NIST un ITIL piemērošanas analīzi, identificējot stiprās un vājās puses. Piedāvā uzlabojumus šo standartu un prakses integrācijā organizācijas drošības politikā.
	2.2. Drošības klases un pakalpojumu klasifikācija.	2.2.1. Drošības klases noteikšana atbilstoši organizācijas vajadzībām. 2.2.2. Pakalpojumu drošības klasifikācija (konfidencialitāte, integritāte, pieejamība). 2.2.3.Datu un informācijas klasifikācija.	Apraksta galvenās drošības klases un to mērķus organizācijas kiberdrošības nodrošināšanā. Atpazīst pakalpojumu klasifikācijas pamatprincipus, piemēram, konfidencialitāte, integritāte un pieejamība. Apraksta datu un informācijas klasifikācijas pamatus. Raksturo, kā konfidencialitāte, integritāte un pieejamība tiek piemērota pakalpojumu klasifikācijā. Apraksta vienkāršu datu un informācijas	Izskaidro drošības klašu noteikšanas kritērijiem, pielāgojot tos organizācijas specifiskajām vajadzībām. Izskaidro pakalpojumu klasifikācijas nozīmi, sasaistot to ar kiberdrošības stratēģiskajiem mērķiem. Izskaidro, kā informācijas klasifikācija ietekmē datu drošības procesus organizācijā Izskaidro, kā drošības klases un pakalpojumu klasifikācija uzlabo resursu pārvaldību un drošības procesus. Izskaidro vienkāršu datu un informācijas klasifikāciju, izmantojot vadlīnijas.	Izvērtē drošības klašu un pakalpojumu klasifikācijas lomu organizācijas kiberdrošības stratēģijas pilnveidošanā. Piedāvā uzlabojumus datu un informācijas klasifikācijas procesiem, ņemot vērā organizācijas riska profilu un resursu pieejamību. Analizē drošības klašu un pakalpojumu klasifikācijas ietekmi uz organizācijas drošības procesiem. Veic vienkāršu datu un informācijas klasifikāciju, izmantojot vadlīnijas.

			klasifikāciju, izmantojot vadlīnijas.		
	2.3. Incidentu klasifikācijas principi	2.3.1. Incidentu kategorijas (piem., tīkla uzbrukumi, datu noplūdes utt.). 2.3.2. Organizācijas pienākumi kiberdrošības jomā. 2.3.3. Incidentu pārvaldības procedūras un dokumentācija.	Apraksta galvenās incidentu kategorijas, piemēram, tīkla uzbrukumus, datu noplūdes un piekļuves pārkāpumus. Apraksta incidentu bīstamības līmeņus un reaģēšanas prioritātes. Raksturo pamata procedūras incidentu pārvaldībai un dokumentēšanai. Raksturo, kā incidentu klasifikācija palīdz prioritizēt reaģēšanas pasākumus. Apraksta incidentu pārvaldības procedūru un dokumentācijas lomu drošības procesā. Veic incidentu dokumentēšanu, izmantojot norādītās vadlīnijas.	Izskaidro dažādu incidentu kategoriju ietekmi uz organizācijas drošību. izskaidro, kā tiek noteikti incidentu bīstamības līmeņi un reaģēšanas prioritātes. Izskaidro incidentu pārvaldības procedūru un dokumentācijas nozīmi. Izskaidro incidentu klasifikācijas sasaisti ar reaģēšanas stratēģijām un resursu efektīvu izmantošanu. Izskaidro incidentu pārvaldības un dokumentācijas nozīmīgumu organizācijas riska pārvaldībā. Veic incidentu dokumentēšanu.	Analizē incidentu klasifikācijas pieejas un to ietekmi uz organizācijas drošības stratēģiju. Novērtē esošo procedūru efektivitāti un piedāvā uzlabojumus incidentu pārvaldības un dokumentēšanas procesā. Analizē incidentu klasifikācijas un pārvaldības ietekmi uz drošības stratēģiju efektivitāti. Analizē klasifikācijas uzlabojumus, reaģēšanas un dokumentācijas procesus, reaģēšanas laika samazināšanai un atbilstības normatīvajām prasībām uzlabošanai. Veic detalizētu incidentu dokumentāciju, ievērojot organizācijas politiku un normatīvos aktus.
	2.4. Standartu ieviešana praksē.	2.4.1. Organizācijas drošības politiku izstrāde un ieviešana.	Apraksta pamatprincipus drošības politiku izstrādei un ieviešanai organizācijās.	Izskaidro drošības politiku lomu organizācijas kiberdrošības stratēģijas.	Analizē drošības politiku izstrādes procesu un piedāvā uzlabojumus,

		2.4.2. Organizācijai piederošie un koplietotie IKT resursi. 2.4.3. Incidentu pārvaldības praktiskie piemēri.	Apraksta galvenos audita un uzraudzības mehānismus, kas nodrošina atbilstību drošības standartiem. raksturo vispārējos incidentu pārvaldības piemērus un to pielietošanu.	Izskaidro audita un uzraudzības mehānismu nozīmi. Salīdzina detalizētus incidentu pārvaldības piemērus un to integrāciju drošības politikā.	balstoties uz labāko praksi. Novērtē audita un uzraudzības mehānismu efektivitāti un izstrādā stratēģiskus ieteikumus to uzlabošanai. Izvērtē incidentu pārvaldības piemērus un izstrādā pielāgotus risinājumus konkrētiem organizācijas riskiem.
	2.5. Kiberdrošības ietvarstruktūru pārskats.	2.5.1. Kiberdrošības ietvari (piemēram, NIST, ESCO, u.c).	Nosauc kiberdrošības profesiju ietvarstruktūras, to lomas un galvenās funkcijas. Definē informācijas sistēmu drošības standartu pamatnosacījumus. Apraksta nepieciešamās komunikācijas prasmes sadarbībā ar dažādu jomu drošības speciālistiem.	Izprot kiberdrošības ietvarstruktūras. Analizē informācijas sistēmu drošības standartu nosacījumus. Izskaidro nepieciešamās komunikācijas prasmes sadarbībā ar dažādu jomu drošības speciālistiem un organizācijas vadītājiem.	Izvērtē un pielāgo kiberdrošības profesiju ietvarstruktūras organizācijas specifiskajām vajadzībām. Izskaidro un piemēro informācijas sistēmu drošības standartus organizācijā. Pamato un pielieto nepieciešamās komunikācijas prasmes sadarbībā ar dažādu jomu drošības speciālistiem, organizācijas darbiniekiem un vadītājiem.
	2.6. Kiberdrošības lomas un atbildības.	2.6.1. Kiberdrošības, tehniķis, analītiķis, arhitekts,	Apraksta kiberdrošības profesionāļu galvenās lomas, piemēram, tehniķa, analītiķa,	Izskaidro kiberdrošības lomu specifiskos pienākumus un to nozīmi organizācijas drošībā.	Analizē kiberdrošības profesionāļu lomu sadarbību un tās ietekmi uz

		pārvaldnieks, vadītājs.	arhitekta, pārvaldnieka un vadītāja funkcijas. Apraksta incidentu reaģēšanas komandas galvenos uzdevumus un sadarbības pamatprincipi. Uzskaita vispārīgas profesionāļu sertifikācijas prasības, piemēram, CISSP, CEH vai CompTIA Security+. Apraksta tehniķu, analītiķu un vadītāju lomu kiberdrošības pārvaldībā. Apraksta incidentu reaģēšanas komandas sadarbības pamatprincipus un to ietekmi uz incidentu pārvaldību.	Izskaidro, kā incidentu reaģēšanas komanda sadarbojas kiberdrošības incidentu efektīvā pārvaldībā. Izskaidro konkrēto sertifikāciju nozīmi un prasības dažādu lomu profesionālajai kvalifikācijai. Izskaidro kiberdrošības lomu mijiedarbības un sadarbības nozīmi incidentu pārvaldībā. Izskaidro, kā konkrētas profesionālās sertifikācijas palīdz paaugstināt drošības speciālistu efektivitāti.	organizācijas drošības stratēģiju. Novērtē sertifikāciju nozīmi profesionālajā attīstībā un piedāvā ieteikumus sertifikācijas izvēlei organizācijas mērķu sasniegšanai. Analizē incidentu reaģēšanas komandas sadarbību un piedāvā uzlabojumus tās efektivitātei. Analizē profesionālo sertifikāciju nozīmi organizācijas drošības stiprināšanā un iesaka uzlabojumus kvalifikācijas prasībās dotajā scenārijā
		2.6.2.Riska mazināšanas stratēģijas un svarīgums. 2.6.3. Profesionāļu sertifikācijas prasības.			
	2.7. Praktiskie scenāriji un simulācijas.	2.7.1. Tehniskās informācijas prezentēšana dažādām iesaistītajām pusēm (vadībai, kolēģiem, sadarbības partneriem, lietotājiem utt.)	Raksturo tehniskās informācijas pielāgošanas pamatprincipus dažādiem auditorijas veidiem, piemēram, vadībai vai lietotājiem. Apraksta normatīvo aktu vispārīgās prasības informācijas sistēmu drošības pārvaldībā. Raksturo starpdisciplināras komandas sadarbības pamatprincipus kiberdrošības incidentu risināšanā.	Izskaidro efektīvas komunikācijas stratēģijas, kas pielāgotas dažādām iesaistītajām pusēm, piemēram, vadībai un sadarbības partneriem. Izskaidro normatīvo aktu detalizētas prasības un to praktisko pielietojumu drošības procesos. Izskaidro organizēšanas un vadības lomu starpdisciplināras komandas sadarbībā incidentu pārvaldībā. Salīdzina tehniskās informācijas pasniegšanas	Novērtē komunikācijas pieejas efektivitāti dažādiem auditorijas līmeņiem un piedāvā uzlabojumus. Piedāvā risinājumus normatīvo aktu integrācijai informācijas sistēmu drošības pārvaldībā. Izstrādā komunikācijas stratēģijas, kas pielāgotas konkrētām auditorijām, piemēram, lietotājiem vai vadībai.
		2.7.2.Efektīva sadarbība ar iekšējiem un ārējiem partneriem.			
		2.7.3.Normatīvo aktu piemērošana informācijas sistēmu drošības pārvaldībā.			

			Apraksta tehniskās informācijas prezentācijas nozīmi un tās pielāgošanu dažādām auditorijām. Apraksta, kā normatīvie akti tiek piemēroti praktiskajā drošības pārvaldībā. Apraksta tehniskās informācijas prezentēšanas veidus dažādām auditorijām.	veidus dažādām auditorijām.	Analizē normatīvo aktu prasības un izstrādā efektīvus to piemērošanas procesus drošības pārvaldībā. Pielāgo un prezentē tehnisko informāciju dažādām auditorijām.
3.Spēj: novērtēt esošo kiberdrošības prasību izpildi informācijas sistēmām, risinājumiem, komponentēm. **Zina:** kiberdrošības saistošā likumdošana un tiesību akti. **Izprot:** tehniskās komponentes, kas veido organizācijas IKT resursus (gan piederošos, gan koplietojamos, gan atsevišķi pārvaldāmos).	3.1. Nacionālā IKT un kiberdrošības likumdošana. 25% no moduļa kopējā apjoma	3.1.1. Nacionālais kiberdrošības likums un saistošie normatīvie akti. 3.1.2.Valsts noteiktā kritiskā IKT infrastruktūra. 3.1.3. Nacionālā drošības koncepcija. 3.1.4. Nacionālās drošības likums. 3.1.5. Elektronisko sakaru likums 3.1.6. Valsts informācijas sistēmu likums 3.1.7. Informācijas sistēmu drošības pārbaudes vadlīnijas.	Apraksta galvenos IKT un kiberdrošības normatīvos aktus un to nozīmi kiberdrošības politikas veidošanā. Apraksta katra normatīvā akta pamatprincipus un to ietekmi uz kiberdošības pasākumiem, atšķir normatīvo aktu nozīmi dažādās organizācijas darbības jomās. Veic vienkāršu organizācijas drošības atbilstību normatīvo aktu prasībām. Atpazīst valsts noteiktās kritiskās IKT infrastruktūras galvenos elementus.	Izskaidro IKT un kiberdrošības normatīvo aktu saturu un mērķus un ietekmi organizācijās procesu nodrošināšanā. Izskaidro normatīvo aktu mijiedarbību kiberdrošības nodrošināšanā. Salīdzina normatīvo aktu prasības dažādām organizācijām. Izskaidro kritiskās IKT infrastruktūras galvenās kategorijas un to lomu valsts drošības nodrošināšanā.	Analizē IKT un kiberdrošības normatīvos aktus un to ietekmi organizācijas kiberdrošības stratēģijas veidošanā. Analizē normatīvo aktu saistību ar organizācijas drošības politikām. Pielieto normatīvo aktu prasībās dažādu organizāciju drošības prasībām. Analizē kritiskās IKT infrastruktūras stratēģisko nozīmi un tās lomu valsts drošības politikā.
	3.2. Eiropas direktīvas un standarti	3.2.1. Eiropas savienības direktīvas (VDAR, NIS2).	Apraksta galvenās ES direktīvas un starptautiskos standartus.	Izskaidro galvenās direktīvu prasības organizācijas drošības stratēģijā un standartu	Analizē ES direktīvu un starptautisko standartu ietekmi organizācijas

		3.2.2. Straptautiskie standarti (ISO 27001, NIST *Cybersecurity Framework*).	Apraksta direktīvu nozīmi datu aizsardzībā un incidentu pārvaldībā. Veic vienkāršu analīzi organizācijas atbilstībai direktīvu un standartu prasībām, vadoties pēc iepriekš sagatavotiem norādījumiem	pielietojumu organizācijas drošības pārvaldības uzlabošanā. Izskaidro direktīvu nozīmi datu aizsardzībā un incidentu pārvaldībā. Izskaidro analīzes rezultātus atbilstībai direktīvu un standartu prasībām.	kiberdrošības prasību īstenošanā. Analizē direktīvu nozīmi datu aizsardzībā un incidentu pārvaldībā. Patstāvīgi veic organizācijas atbilstības novērtējumu direktīvu un standartu prasībām.
	3.3. Juridiskās sankcijas un atbildība.	3.3.1. Sodi un sekas par neatbilstība kiberdrošības prasībām. 3.3.2. Organizācijas pienākumi kiberdrošības jomā.	Apraksta sodus un sankcijas neatbilstībai kiberdrošības prasībām. Apraksta organizācijas vispārīgos pienākumus kiberdrošības jomā. Apraksta, kāpēc organizācijām ir svarīgi ievērot normatīvajos aktos noteiktos kiberdrošības pienākumus. Sagatavo vienkāršu pārskatu par juridiskajiem riskiem un pienākumiem, izmantojot dotos materiālus.	Izskaidro juridiskās sekas normatīvo aktu pārkāpumiem kiberdrošībā, to ietekmi uz organizācijas reputāciju un darbību. Izskaidro organizāciju pienākumus kiberdrošības jomā. Izskaidro organizācijas rīcību pienākumu izpildē kiberdrošības jomā, lai izvairītos no juridiskām sankcijām. Izstrādā darbības plānu, lai nodrošinātu organizācijas pienākumu izpildi kiberdrošības prasībām.	Analizē sodu piemērošans principus un no tā izrietošās sekas. Izveido organizācijas pienākumu sarakstu kiberdrošības jomā dažādām organizācijām. Analizē praktiskus piemērus organizācijas rīcībai pienākumu izpildē kiberdrošības jomā. Analizē stratēģiskus risinājumus organizācijas juridiskās atbilstības pilnveidošanā un iespējamo sodu un sankciju novēršanā.
	3.4.Organizācijas IKT resursu klasifikācija	3.4.1. IKT komponenšu kataloga veidošana un anlīze	Apraksta organizācijas IKT resursu veidus, tai skaitā piederošos un koplietotos resursus.	Izskaidro IKT resursu klasifikācijas principus un to pielietojumu organizācijas pārvaldības procesos.	Analizē IKT resursu klasifikācijas un komponenšu kataloga nozīmi organizācijā

		3.4.2. Organizācijai piederošie un koplietotie IKT resursi.	Apraksta IKT komponenšu kataloga galvenos elementus un tā nozīmi IKT pārvaldībā. Apraksta kā resursu klasifikācija palīdz identificēt un pārvaldīt IKT resursus. Uzskaita pamata resursus, identificējot piederošos un koplietotos resursus.	Izskaidro IKT komponenšu kataloga veidošanu un izmantošanu. Izskaidro kā klasifikācijas sistēmas uzlabo organizācijas resursu izmantošanu un atbilstību drošības standartiem. Klasificē resursus.	Analizē organizācijas komponenšu kataloga ietekmi atbilstoši organizācijas vajadzībām. Analizē klasifikācijas ietekmi uz organizācijas drošības standartiem. Izveido komponenšu katalogu atbilstoši organizācijas vajadzībām.
	3.5. Kiberdrošības prasību identifikācija un novērtēšana.	3.5.1. Normatīvo aktu un vadlīniju pārskats. 3.5.2. Organizācijas specifisko kiberdrošības prasību noteikšana.	Apraksta galvenos normatīvos aktus un vadlīnijas. Definē normatīvo aktu un vadlīniju lomu organizācijas drošības prasību izstrādē. Sakārto pamata normatīvo aktu un vadlīniju pārskatu.	Izskaidro galveno normatīvo aktu un vadlīniju saturu un mērķus. Salīdzina normatīvos aktus ar organizācijas kiberdrošības procesiem un politiku, Analizē normatīvo aktu un vadlīniju ietekmi organizācijas kiberdrošības prasībām.	Analizē normatīvos aktus un vadlīnijas, sasaistot tos ar organizācijas drošības prasībām. Analizē normatīvos aktus un vadlīnijas organizācijas iespējamo risku un trūkumu identificēšanai. Analizē stratēģiskus risinājumus un ieteikumus organizācijas drošības procesu veicināšanai.
	3.6. Prasību novērtēšanas process.	3.6.1. Informācijas sistēmu un risinājumu audita metodes. 3.6.2. Atbilstības pārbaudes un dokumentēšana.	Apraksta galvenās informācijas sistēmu audita metodes un atbilstības pārbaudes posmus. Atpazīst scenāriju izstrādes pamatprincipi prasību novērtēšanai.	Izskaidro informācijas sistēmu audita metodes un to nozīmi kiberdrošības prasību pārbaudē. Izskaidro atbilstības pārbaudes procesu un dokumentācijas lomu	Analizē audita metožu un atbilstības pārbaudes procesu efektivitāti organizācijas drošības politikā. Izvērtē uzlabojumu scenārijus efektīvu

		3.6.3. Scenāriju izstrāde prasību novērtēšanai un ieviešanai.	Apraksta informācijas sistēmu audita lomu prasību atbilstības novērtēšanā.	drošības prasību ievērošanā. izskaidro audita un atbilstības pārbaudes procesu sasaisti ar organizācijas drošības politiku.	drošības prasību novērtēšanai un ieviešanai. Analizē prasību novērtēšanas procesu saistībā ar organizācijas stratēģiskajiem mērķiem.
4.Spēj: apzināt atšķirības starp dažādu kiberdrošības profesiju, kiberdrošības lomu, pienākumiem un atbildībām. **Zina:** Latvijas kiberdrošības atbildīgo institūciju hierarhija un to uzdevumi. **Izprot:** normatīvo regulējuma prasības un to nozīmi organizācijas kiberdrošības nodrošināšanā.	4.1. Latvijas kiberdrošības institūcijas. 25% no moduļa kopējā apjoma	4.1.1. Nacionālās kiberdrošības centrs, uzdevumi, pilnvaras, funkcijas. 4.1.2. CERT.lv, uzdevumi, pilnvaras, funkcijas. 4.1.3. Aizsardzības ministrijas un Nacionālo bruņoto spēku loma kiberdrošībā. 4.1.4. Datu valsts inspekcija.	Nosauc Latvijas kiberdrošības atbildīgo institūciju hierarhiju un to uzdevumus. Raksturo normatīvo regulējumu prasības un to nozīmi organizācijas kiberdrošības nodrošināšanā. Skaidro atšķirības starp dažādām kiberdrošības profesijām, kiberdrošības lomām, pienākumiem un atbildībām.	Izskaidro Latvijas kiberdrošības atbildīgo institūciju hierarhiju un to uzdevumus. Apraksta un pamato normatīvo regulējumu prasības un to nozīmi organizācijas kiberdrošības nodrošināšanā. Izskaidro atšķirības starp dažādu kiberdrošības profesiju, kiberdrošības lomu pienākumiem un atbildībām.	Izprot un izskaidro Latvijas kiberdrošības atbildīgo institūciju hierarhiju un to specifiskos uzdevumus. Patstāvīgi izvēlas un pielieto normatīvo regulējumu prasības organizācijas kiberdrošības nodrošināšanā. Izvērtē un izskaidro dažādu kiberdrošības profesiju atšķirības, lomas, pienākumus un atbildības
	4.2. Institūciju hierarhija un sadarbība.	4.2.1.Institūciju hierarhija. 4.2.2.Institūciju sadarbība kritiskās infrastruktūras aizsardzībā. 4.2.3.Krīžu vadība un incidentu reaģēšanas protokoli	Apraksta galvenās kiberdrošības institūcijas un to hierarhisko struktūru. Apraksta sadarbības pamatprincipus starp institūcijām kritiskās infrastruktūras aizsardzībā. Apraksta pamatprincipus krīžu vadības un incidentu reaģēšanas protokolu izstrādē un piemērošanā.	Izskaidro kiberdrošības institūciju lomu un hierarhijas nozīmi drošības koordinācijā Izskaidro institūciju sadarbības nozīmi efektīvas kritiskās infrastruktūras aizsardzībā. Izskaidro krīžu vadības protokolu sasaisti ar institūciju hierarhiju un sadarbību.	Analizē institūciju hierarhijas efektivitāti. Novērtē sadarbības modeļu nozīmi un to ietekmi uz kritiskās infrastruktūras aizsardzības pasākumiem. Analizē krīžu vadības un incidentu reaģēšanas protokolu efektivitāti.

			Apraksta, kā institūcijas sadarbojas krīzes situācijās, lai nodrošinātu infrastruktūras drošību. Veic vienkāršu incidentu reaģēšanas protokola analīzi un pielietošanu praksē.	Izskaidro galvenos incidentu reaģēšanas protokola elementus un to nozīmi efektīvā sadarbībā. Izskaidro incidentu reaģēšanas protokolus, pamatojoties uz organizācijas specifiskajām vajadzībām.	Analizē institūciju sadarbības pasākumus krīžu vadības un reaģēšanas procesu uzlabošanā. Izveido incidentu reaģēšanas protokolus, pamatojoties uz organizācijas specifiskajām vajadzībām.
	4.3. Starptautiskas organizācijas un sadarbība.	4.3.1.ENISA. 4.3.2.Eiropas Savienības iniciatīvas 4.3.3.Starptautiskie sadarbības tīkli (piem, FIRST).	Apraksta galvenās starptautiskās organizācijas, piemēram, ENISA un FIRST, un to lomu kiberdrošībā. Apraksta Eiropas Savienības kiberdrošības iniciatīvas un to mērķus. Apraksta ENISA un globālo sadarbības tīklu, piemēram, FIRST, lomu drošības uzlabošanā un informācijas apmaiņā.	Izskaidro ENISA darbības jomu un galvenos uzdevumus kiberdrošības veicināšanā Eiropā. Izskaidro konkrētas Eiropas Savienības iniciatīvas un to nozīmi dalībvalstu kiberdrošības uzlabošanā. Salīdzina ENISA un Eiropas iniciatīvas ar organizācijas kiberdrošības pasākumiem.	Analizē starptautisko organizāciju, piemēram, FIRST, nozīmi globālajā sadarbībā un incidentu pārvaldībā. Novērtē Eiropas Savienības kiberdrošības iniciatīvu ietekmi uz organizācijas drošības stratēģijām un regulām. Analizē starptautisko organizāciju un sadarbības tīklu efektivitāti kiberdrošības apdraudējumu risināšanā un sadarbības uzlabošanā.
	4.4. Normatīvo aktu prasību piemērošana praksē.	4.4.1.Organizācijas iekšējās kiberdrošības politikas izstrāde.	Apraksta galvenās normatīvo aktu prasības, kas attiecas uz	Izskaidro normatīvo aktu prasību piemērošanu organizācijas	Analizē normatīvo aktu prasību ietekmi uz organizācijas

		4.4.2.Audita un atbilstības pārbaudes metodes. 4.4.3.Sankciju un atbildības riski normatīvo aktu pārkāpumu gadījumā.	organizācijas kiberdrošību. Uzskaita audita un atbilstības pārbaudes vispārējās metodes. Apraksta normatīvo aktu ietekmi organizācijas kiberdrošības politikas veidošanā. Apraksta sankciju un atbildības riskus, kas izriet no normatīvo aktu prasību pārkāpumiem. Apraksta vienkāršu organizācijas iekšējo kiberdrošības politiku, izmantojot vadlīnijas un normatīvo aktu prasības. Apraksta pamata audita un atbilstības pārbaudes, balstoties uz sniegtajiem norādījumiem.	kiberdrošības politikas izstrādē. Izskaidro audita un atbilstības pārbaudes metožu nozīmi organizācijas drošības procesā. Sasaista normatīvo aktu prasības ar organizācijas iekšējās drošības politikas mērķiem. Izskaidro, kā audita un atbilstības pārbaudes procesi palīdz mazināt sankciju un atbildības riskus. izskaidro vienkāršu organizācijas iekšējo kiberdrošības politiku, izmantojot vadlīnijas un normatīvo aktu prasības. Apraksta pamata audita un atbilstības pārbaudes, balstoties uz sniegtajiem norādījumiem.	kiberdrošības stratēģiju. Analizē audita metožu un atbilstības pārbaudes procesu efektivitāti. Analizē normatīvo aktu prasību pārkāpuma sekas. Novērtē organizācijas kiberdrošības politikas atbilstību normatīvajiem aktiem un piedāvā uzlabojumus. Izstrādā vienkāršu organizācijas iekšējo kiberdrošības politiku, pielietojot vadlīnijas un normatīvo aktu prasības. Veic pamata audita un atbilstības pārbaudes, dotajā scenārijā.
	4.5. Normatīvo aktu un tehnoloģiju savienojamība.	4.5.1. Normatīvo aktu ietekme drošības rīku ieviešanā. 4.5.2. Labās prakses piemēri normatīvo aktu integrācijā tehnoloģiju ieviešanā.	Apraksta galvenos normatīvos aktus, kas ietekmē drošības rīku ieviešanu organizācijās. Nosauc pamata labās prakses piemēri normatīvo aktu integrācijā tehnoloģiju ieviešanā. Apraksta, kā normatīvie akti nosaka drošības rīku izvēli un ieviešanas prasības. Apraksta labās prakses piemērus, lai atbilstu	Izskaidro normatīvo aktu prasību nozīmi drošības rīku ieviešanas procesā. Izskaidro konkrētus labās prakses piemērus normatīvo aktu un tehnoloģiju integrācijas jomā. Izskaidro normatīvo aktu un tehnoloģiju integrācijas nozīmi drošības stratēģiju izveidē. Salīdzina labās prakses piemērus, lai atbilstu	Analizē normatīvo aktu prasību ietekmi uz drošības tehnoloģiju izvēli un ieviešanu organizācijā. Novērtē labās prakses piemēru efektivitāti un sniedz ieteikumus to pielāgošanai konkrētās situācijās. Analizē normatīvo aktu un tehnoloģiju savienojamības ietekmi uz drošības

			normatīvajām prasībām tehnoloģiju ieviešanā.	normatīvajām prasībām tehnoloģiju ieviešanā.	stratēģijas efektivitāti. Veic atbilstības pārbaudes, lai novērtētu normatīvo prasību un tehnoloģiju integrācijas efektivitāti, atbilstoši iepriekš dotam scenārijam.
	4.6. Kiberdrošības profesiju pārskats.	4.6.1.Dažādu kiberdrošības profesiju pārskats,nepieciešamās prasmes un zināšanas. 4.6.2.Sadarbība starp dažādām kiberdrošības lomām 4.6.3. Jaunas prasmes un profesijas (piem. MI drošības analītiķis). 4.6.4.Sertifikāciju un kvalifikācijas nozīme.	Apraksta galvenās kiberdrošības profesijas un to pamatfunkcijas. Apraksta prasības un sertifikācijas, kas nepieciešamas dažādām lomām, piemēram, CISSP vai CEH. Definē sadarbības nozīmi starp dažādām kiberdrošības lomām, piemēram, tehniķiem, analītiķiem un vadītājiem. Apraksta jauno profesiju, piemēram, MI drošības analītiķa, lomu kiberdrošības kontekstā. Apraksta vienkāršus sadarbības plānus starp dažādām kiberdrošības lomām	Izskaidro dažādu kiberdrošības profesiju specifiskās prasmes un lomas organizācijā. Izskaidro sertifikāciju nozīmi profesionālās kvalifikācijas celšanā un karjeras attīstībā. Izskaidro efektīvas sadarbības principus starp dažādām kiberdrošības lomām organizācijas mērķu sasniegšanā. Izskaidro, kā jauno prasmju un profesiju attīstība atbilst mainīgajai kiberdrošības videi. Izskaidro vienkāršus sadarbības plānus starp dažādām kiberdrošības lomām	Analizē kiberdrošības profesiju savstarpējo saistību un to ieguldījumu organizācijas drošības stratēģijā. Piedāvā rekomendācijas sertifikāciju izvēlei un profesionālajai attīstībai, balstoties uz organizācijas mērķiem. Analizē sadarbības efektivitāti starp dažādām kiberdrošības lomām. Novērtē jauno prasmju un profesiju stratēģisko nozīmi organizācijas drošības stiprināšanā. Izveido vienkāršus sadarbības plānus starp dažādām kiberdrošības lomām

Izmantotie avoti:

1. Autoru grupa Informācijas sabiedrības tiesību pamati, izd. Rīgas Stradiņa universitāte, Rīga, 2022., 679.lpp
2. Nacionālās kiberdrošības likums, https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums

3. Nacionālās drošības koncepcija, https://likumi.lv/ta/id/309647-par-nacionalas-drosibas-koncepcijas-apstiprinasanu
4. Nacionālās drošības likums, https://likumi.lv/ta/id/14011-nacionalas-drosibas-likums
5. Latvijas kiberdrošības stratēģija 2023.-2026.gadam, https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABbas%20strat%C4%93%C4%A3ija%202023.-2026.gadam .pdf
6. Elektronisko sakaru likums, https://likumi.lv/ta/id/334345
7. Valsts informācijas sistēmu likums, https://likumi.lv/doc.php?id=62324
8. Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (Dokuments attiecas uz EEZ), https://eur-lex.europa.eu/eli/dir/2022/2555/oj/?locale=LV
9. https://www.enisa.europa.eu/

MODUĻA Incidentu klasifikācija, reaģēšana, analīze, novēršana APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmes incidentu klasifikācijā un apstrādē.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses; veikt kiberdrošības incidentu reģistrēšanu; veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām. 2. patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem. 3. patstāvīgi veikt incidentu apstrādi (reģistrēšanu, izpēti, ietekmes novērtēšanu atbilstoši organizācijas norādījumiem).
Moduļa ieejas nosacījumi	Apgūti A daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudes darbu, kurā ir teorētisko zināšanu pārbaudes jautājumi im praktiskais uzdevums- veikt incidentu apstrādi, atbilstoši dotajam scenārijam.
Moduļa nozīme un vieta kartē	Modulis " Incidentu klasifikācija, reaģēšana, analīze, novēršana " ir B daļas modulis. To apgūst vienlaicīgi ar moduli "IKT un kiberdrošības normatīvo aktu piemērošana". Pēc moduļa apguves seko moduļa "IS drošības inženierija , IS stiprināšana, konfiigurācijas uzturēšana" apguve.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Incidentu klasifikācija, reaģēšana, analīze, novēršana SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis*
1.Spēj: identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses; veikt kiberdrošības incidentu reģistrēšanu; veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām. **Zina:** incidenta dzīvesciklu (tā sastāvdaļas - priekšizpētei nepieciešamo informāciju). **Izprot:** incidentu apstrādes standarti, labā prakse, digitālās izmeklēšanas nozīme.	1.1.Kiberdrošības incidentu identificēšana 8% no moduļa kopējā apjoma	1.1.1.Incidenta definīcija un to veidi	1.1.Atpazīst izplatītākos incidentu veidus (piemēram, ļaunatūra, DoS, datu noplūde) pēc nosaukuma. Prot sniegt vienkāršus piemērus dažādiem incidentu veidiem	1.1.Pārzina būtiskās atšķirības starp incidentu veidiem, kritiski izvērtē konkrētu situāciju un nosauc iespējamo incidentu kategoriju.	1.1.Analizē kiberdrošības incidentu definīciju dažādos kontekstos (tehniskais, juridiskais, organizatoriskais). Piemēro zināšanas par incidentu veidiem, piedāvājot ieteikumus iespējamo risku vadībai
		1.1.2.Identificēšanas metodes un rīki	Nosauc rīkus un metodes kiberdrošības incidentu atklāšanai (antivīrusi, IDS/IPS, žurnālu analīze) Veic vienkāršu sistēmas un notikumu žurnāla pārbaudi, lai konstatētu acīmredzamas aizdomīgas pazīmes	Izvēlas atbilstošus rīkus konkrētu incidentu atklāšanai. Analizē notikumu žurnālus, izceļot anomālijas un definējot noteikumus brīdinājumu konfigurācijai Izmanto vairākas metodes un spēj pamatot, kāpēc konkrēta metode/rīks ir efektīvs noteiktos gadījumo	Izstrādā jaunas vai pielāgo esošās identificēšanas metodes, iekļaujot sarežģītāku draudu izlūkošanu (threat intelligence) Novērtē un konfigurē modernus un integrētus risinājumus organizācijas vajadzībām. Optimizē incidentu atklāšanas procesu, novēršot nepilnības un sagatavojot ilgtermiņa stratēģiju

		1.1.3.Ietekmēto resursu noteikšana	Nosauc organizācijai svarīgākos IT resursus (serveri, datubāzes, tīkls, lietojumprogrammas). Atpazīst pamatpazīmes, kas liecina par konkrēta resursa ietekmēšanu (piemēram, negaidīti servisa pārtraukumi, dīvaina tīkla datu plūsma). Dokumentē ietekmēto resursu pamatinformāciju (nosaukums, atrašanās vieta, atbildīgā persona	Kritiski izvērtē notikuša incidenta ietekmi uz dažādiem resursiem, tostarp datiem un lietojumprogrammām. Izmanto rīkus un datu analīzi, lai noteiktu incidenta apmēru un iespējamo seku nopietnību.	Izstrādā un ievieš procesus un politikas, kas ļauj strukturēti un ātri noteikt ietekmētos resursus lielās, kompleksās organizācijās. Veic padziļinātu risku analīzi un izstrādā ieteikumus resursu aizsardzības prioritātēm saskaņā ar biznesa vajadzībām. Demonstrē stratēģisku skatījumu, paredzot potenciālo ietekmi arī uz saistītajiem/ārējiem resursiem un biznesa procesiem.
		1.1.4.Iesaistītās puses un to lomas	Nosauc galvenos dalībniekus incidentu pārvaldībā (IT drošības speciālisti, vadība, trešās puses, tiesībsargājošās iestādes) Apraksta katra dalībnieka vispārīgo atbildības jomu (piemēram, IT drošības speciālists veic tehnisko analīzi) Pārzina bāzes principus, kad nepieciešams kontaktēties ar konkrētu iesaistīto pusi.	Piedalās incidentu reaģēšanas komandā, sadalot lomas un atbildības, lai nodrošinātu efektīvu sadarbību Uztur komunikāciju starp iesaistītajām pusēm, definējot eskalācijas ceļus un informācijas apmaiņas kārtību. Izprot juridisko un normatīvo prasību ietekmi uz komunikācijas plūsmu un pienākumu ziņot noteiktām iestādēm	Izstrādā stratēģisku sadarbības modeli starp iekšējo drošības komandu, vadību un ārējiem partneriem/ plāno un vēršas pie attiecīgajām iestādēm krīzes situācijā, nodrošinot uzņēmuma interešu pārstāvību un tiesisko atbilstību

	1.2. Kiberdrošības incidentu reģistrēšana 8% no moduļa kopējā apjoma	1.2.1.Reģistrācijas un informācijas vākšanas process	Prot atkārtot reģistrācijas procesa pamatsoļus. Atpazīst, kādi dati ir būtiski sākotnējo ziņojumu veidošanai (kur, kad, kā incidents notika). Spēj aprakstīt vienkāršas procedūras, kā tiek vākti incidenta sākotnējie pierādījumi (žurnālu fragmenti, ekrānšāviņi).	Veido strukturētu incidentu reģistrācijas ierakstu, sistemātiski apkopo un kategorizē informāciju (laiks, iesaistītās sistēmas, ietekmētās funkcijas). Demonstrē spēju plānot un organizēt informācijas vākšanu, iekļaujot dažādus avotus (žurnālu analīze, lietotāju atskaites, tīkla monitorings). Pielāgo reģistrācijas procesu atkarībā no incidenta veida un organizācijas specifikas (piem., ievērojot uzņēmuma politikas vai regulatora prasības).	Izmato visaptverošus informācijas vākšanas standartus un procedūras, kas aptver gan tehniskos, gan organizatoriskos aspektus. Kritiski izvērtēt reģistrācijas un vākšanas procesā iegūtos datus, identificējot nepilnības un ierosinot uzlabojumus. Nodrošina, ka reģistrēšanas process ir pietiekami detalizēts un elastīgs, lai būtu izmantojams digitālās izmeklēšanas analīzē un atbilstu normatīvajām prasībām.
		1.2.2.Reģistrācijas rīki un platformas	Nosauc galvenos rīkus un platformas, kurās var reģistrēt incidentus (piem., vienkāršas izklājlapas, Helpdesk sistēmas, e-pasts, bāzes ITSM risinājumi). Pārzina pamata funkcionalitāti (incidentu reģistrēšana, statusu maiņa, pamatinformācijas saglabāšana). Var pieslēgties jau esošai reģistrācijas	Patstāvīgi izvēlas vai konfigurē piemērotu reģistrācijas rīku, pamatojoties uz incidenta kritiskumu un organizācijas vajadzībām. Demonstrē spēju integrēt incidentu reģistrācijas platformu ar citiem risinājumiem (SIEM, monitoringa sistēmas) vienotai informācijas apmaiņai. Novērtē dažādu rīku vai platformu plusus un	Projektē un ievieš sarežģītu incidentu pārvaldības risinājumu ekosistēmu (integrētas ITSM, SOAR, SIEM un citus rīkus). Izstrādā papildu funkcionalitāti vai spraudņus (plugins), lai paplašinātu standarta platformu iespējas, piemēram,

			platformai un ievadīt tajā nepieciešamos datus.	mīnusus, ieteicot atbilstošāko risinājumu savā darba vidē.	automātisko incidentu klasifikāciju. Veicina inovācijas, piemēram, mašīnmācīšanās vai lielo datu analīzes integrāciju, lai optimizētu incidentu reģistrācijas un reaģēšanas laiku.
		1.2.3.Pierādījumu iegūšana un to integritātes saglabāšana.	izskaidro nepieciešamību pierādījumu iegūšanai incidenta laikā (piem., lai noteiktu uzbrukuma vektoru vai vainīgo personu). Atpazīst pamata drošības pasākumus, kas jāievēro, lai pierādījumi netiktu mainīti (kopiju izveide, failu "hash" pārbaude). Dokumentē iegūto materiālu (logu failus, ekrānattēlus) atbilstoši vienkāršām norādēm.	Veic digitālās kriminalistikas drošības pasākumus, piemēram, datu nesēja klona izveidi (imaging), pierādījumu "hash" kalkulāciju un verifikāciju. Pārvalda starptautiski atzītus rīkus un metodes (EnCase, FTK u.c.), nodrošinot, ka pierādījumu ķēdes (chain of custody) prasības tiek ievērotas. Skaidri komunicē un nodrošinā atbildīgajām pusēm (vadībai, juristiem u.c.) pierādījumu autentiskumu un integritāti	Izstrādā, ievieš un uzrauga visaptverošu digitālās kiminalistikas procedūru sistēmu, lai nodrošinātu neatkārtojamu pierādījumu iegūšanu un saglabāšanu. Veic sarežģītu izmeklēšanas procesu, kas aptver vairākas platformas un ārējos resursus, saglabājot pierādījumu integritāti un gatavojot tos tiesvedībai.
	1.3. Kiberdrošības incidentu ziņošana 10% no moduļa kopējā apjoma	1.3.1.Iekšējā un ārējā ziņošana, incidentu eskalācijas līmeņi.	Uzskaitīt pamatsoļus iekšējai ziņošanai (kam un kad jāpaziņo par konstatēto incidentu). Prot skaidri pateikt, kādi eskalācijas līmeņi pastāv konkrētajā organizācijā (piemēram, speciālists -> nodaļas vadītājs ->	Sastāda incidentu eskalācijas plānu atbilstoši notikuma raksturam un kritiskumam, norādot katrā līmenī iesaistāmās puses. Demonstrē spēju novērtēt, kādu informāciju drīkst un	Ievieš visaptverošu iekšējās un ārējās ziņošanas politiku, kas ietver eskalācijas kārtību atbilstoši dažādu incidentu riska līmeņiem. Var veikt stratēģisku lēmumu pieņemšanu, nosakot, kādas sekas

			drošības komanda -> valdes līmenis). Atpazīst pamatatšķirību starp ziņošanu iekšēji (kolēģiem, tiešajiem vadītājiem) un ārēji (pakalpojumu sniedzējiem, klientiem), bet nespēj to padziļināti analizēt.	vajag komunicēt ārēji (piemēram, klientiem, partneriem), lai nodrošinātu sabalansētu caurspīdīgumu un drošības intereses. Izprot organizācijas iekšējo struktūru, skaidri definējot, kad nepieciešama tūlītēja eskalācija, lai mobilizētu vadības uzmanību un resursus.	var radīt lieks informācijas atklājums un kā saglabāt līdzsvaru starp operatīvo reaģēšanu un konfidencialitāti. Nodrošina, ka eskalācijas plāni ir integrēti plašākā organizācijas krīzes vadības sistēmā, regulāri tos pārskata, testē un pilnveido.
		1.3.2.Nacionālo un starptautisko iestāžu loma.	Pārzina galvenās nacionālās iestādes, kas atbild par kiberdrošības incidentu uzraudzību un koordināciju (piem., CERT). Atpazīst, kādos gadījumos var būt jāziņo par incidentu ārējām uzraugošajām vai tiesībsargājošajām iestādēm. Prot nosaukt dažus starptautiskos sadarbības mehānismus (piem., Eiropas Savienības NIS direktīva).	Patstāvīgi nosaka, kurām nacionālajām vai starptautiskajām institūcijām ir jāziņo konkrētos incidentu scenārijos (GDPR pārkāpumi, kritiskā infrastruktūra u.c.). Demonstrē izpratni par starptautisko normatīvo aktu un vadlīniju (piem., NIS2, ENISA rekomendācijas) ietekmi uz uzņēmuma kiberdrošības praksēm. Uztur sadarbību ar atbildīgajām iestādēm, spējot organizēt nepieciešamo informācijas un zināšanu apmaiņu (piem., dalība kopīgos drošības uzlabošanas pasākumos).	Veido un koordinē organizācijas iekšējo politiku, kas nodrošina savlaicīgu un pilnīgu sadarbību ar nacionālajām un starptautiskajām drošības un regulējošām iestādēm. Piedalās starptautiskus kiberdrošības sadarbības projektus un iniciatīvas, veicinot labās prakses apmaiņu un standartizāciju.
		1.3.3.Informācijas aprite, krīzes komunikācija.	Izprot pamata krīzes komunikācijas nozīmi, spējot sniegt faktus par	Patstāvīgi formulē gan iekšējās, gan ārējās komunikācijas ziņojumus,	Ieviešun regulāri testē organizācijas krīzes komunikācijas

			notikušo incidentu tiešajiem vadītājiem vai kolēģiem. Atpazīst kritiskos kanālus informācijas apritei (e-pasts, ziņojumapmaiņa, intranets). Sagatavo vienkāršu paziņojumu darbiniekiem vai atbildēt uz pamatjautājumiem no ārējiem interesentiem.	ņemot vērā incidenta nopietnību un auditoriju (vadība, darbinieki, klienti, plašsaziņas līdzekļi). Demonstrē gatavību reaģēt uz krīzes situāciju, spējot ātri izveidot komunikācijas plānu un koordinēt tā realizāciju ar atbilstošajiem departamentiem. Mazina reputācijas riskus, precīzi un savlaicīgi sniedzot informāciju un sadarbojoties ar sabiedrisko attiecību vai mārketinga komandām.	stratēģiju, iekļaujot skaidri definētus ziņojumu sagatavošanas un apstiprināšanas procesus. Izvērš kompleksu komunikācijas kampaņu, kas aptver iekšējās struktūrvienības, sabiedriskos medijus, klientus un citas ieinteresētās puses, lai mazinātu incidenta sekas un atjaunotu uzticību. Izvērtē notikumu gaitu, maina un optimizē komunikācijas plānu atbilstoši jauniem apstākļiem, nodrošinot organizācijas vienotu tēlu un interešu aizstāvību.
2.Spēj: patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem. **Zina:** incidentu apstrādes rīki. Incidentu klasifikācijas ietvari, nosacījumi. **Izprot**: risku, draudu, ievainojamību klasifikācija.	2.1.Kiberdrošības Incidentu klasifikācija 10% no moduļa kopējā apjoma	2.1.1.Klasifikācijas mērķi.	Nosauc galvenos iemeslus, kādēļ kiberdrošības incidentus nepieciešams klasificēt (piem., skaidra pārskatāmība, atbilstoša resursu piesaiste). Izprot vienkāršā līmenī, ka klasifikācija palīdz prioritizēt un strukturēt incidentu pārvaldību. Atkārto pamatmērķus no dotām vadlīnijām vai	Paskaidro, kā klasifikācija kalpo par pamatu efektīvai incidentu pārvaldībai (pareizai reaģēšanas komandas iesaistei, ietekmes novērtēšanai u.c.). Pielāgo klasifikācijas mērķus konkrētai organizācijas videi (piem., atbilstoši uzņēmuma biznesa procesiem, normatīvajām prasībām).	Veido un ievieš integrētu klasifikācijas sistēmu, kas precīzi atbilst organizācijas vajadzībām un ilgtermiņa drošības mērķiem. Pamato, kāpēc noteikti klasifikācijas mērķi ir izšķiroši, piemēram, lai samazinātu incidentu

			mācību materiāla, bet pats vēl neveido klasifikācijas sistēmu.	Kritiski izvērtē, kāds ir klasifikācijas ieguldījums drošības stratēģiskajā plānošanā, un iesaka uzlabojumus esošajai pieejai.	izmeklēšanas laiku vai aizsargātu kritisko infrastruktūru. Demonstrē stratēģisku skatījumu: pārzina globālas labās prakses un spēj tās adaptēt savas organizācijas kontekstā, iekļaujot gan tehnisko, gan biznesa perspektīvu.
		2.1.2.Klasifikācijas principi un kritēriji.	Atkārto galvenos klasifikācijas principus (piem., pēc ietekmes līmeņa, pēc tehniskā vektora, pēc uzbrukuma tipa). Nosauc dažus populārus kritērijus (konfidencialitātes pārkāpums, pieejamības samazināšanās u.c.). Izmanto jau definētus kritērijus (piem., no organizācijas drošības rokasgrāmatas/politikas/ procedūrām), nepaplašinot vai nemainot tos pēc savas iniciatīvas.	Pielieto vairākus klasifikācijas principus (piemēram, ietekme uz uzņēmuma reputāciju, atbilstība normatīvajām prasībām) vienas situācijas novērtējumā. Kritiski izvērtē, kurš kritēriju kopums vislabāk atbilst konkrētam incidenta tipam, un pielāgo to, ņemot vērā uzņēmuma darbības specifiku. Demonstrē spēju sasaistīt klasifikācijas principus ar reālu rīcības plānu (piem., kāds ir nākamais solis, ja incidents atbilst noteiktai kritēriju kombinācijai).	Izstrādā un regulāri atjaunina visaptverošu klasifikācijas kritēriju ietvaru (framework), kas ņem vērā gan tehniskos, gan uzņēmējdarbības un regulatīvos aspektus. nodrošina, ka klasifikācijas kritēriji tiek efektīvi izmantoti visā organizācijas ekosistēmā (tostarp meitasuzņēmumos, partnerorganizācijās).
		2.1.3.Incidentu prioritāte, incidentu kritiskuma novērtēšana.	Atpazīst atšķirību starp zemas, vidējas un augstas prioritātes incidentiem, norādot dažus vienkāršus kritērijus (piem., cik sistēmas ietekmētas, vai	Patstāvīgi novērtē incidenta kritiskumu, apskatot gan tehniskos (uzbrukuma veids, izmantojamā ievainojamība) gan biznesa aspektus (finanšu	Veido un uztur daudzslāņu incidentu kritiskuma novērtēšanas sistēmu, kas iekļauj skaitliskus (kvantitatīvos) un

			tiek apdraudēti sensitīvi dati). Izmanto organizācijas noteiktos pamatvirzienus (incidenta smaguma pakāpe vai kritiskuma līmenis) bez padziļinātas analīzes. Prot izveidot vienkāršu sarakstu, lai prioritizētu vienas dienas laikā uzkrātos incidentus.	zaudējumi, ietekme uz reputāciju). Var argumentēti aizstāvēt, kāpēc konkrēts incidents ir jāceļ vai jālaiž zemāk prioritātē, ņemot vērā pieejamos resursus un citus paralēlos incidentus. Kritiski izvērtē organizācijas prioritātes noteikšanas metodiku (vai tās atbilst reālajai situācijai), iesakot korekcijas, lai panāktu labāku risku sadalījumu.	aprakstošus (kvalitatīvos) rādītājus. Nodrošina, ka prioritātes noteikšanā ir iestrādāta uz risku bāzēta pieeja, pievēršot uzmanību organizācijas stratēģiskajiem mērķiem un vispārējam drošības stāvoklim. Demonstrē spēju sabalansēt akūtu incidentu reakciju ar ilgtermiņa drošības uzlabošanu, efektīvi pārvaldot resursus pat lielā mērogā (starptautiskos uzņēmumos, kritiskās infrastruktūras organizācijās).
	2.2. Incidentu klasifikācijas ietvari 8% no moduļa kopējā apjoma	2.2.1.NIST 800-61, ISO 27035.	Atpazīst galvenos jēdzienus un terminoloģiju no NIST SP 800-61 un ISO 27035 (piem., incidentu izmeklēšanas fāzes, incidentu reakcijas dzīves cikls). Nosauc pamatsoļus incidentu pārvaldībā (sagatavošana, atklāšana, ierobežošana, atkopšana, mācīšanās) atbilstoši šo standartu rekomendācijām.	Piemēro NIST 800-61 un/vai ISO 27035 ieteiktās fāzes un darbības soļus konkrētam kiberdrošības incidentam, piemēram, spēj izstrādāt reaģēšanas plānu, kurā iekļauts sagatavošanās, identificēšanas, ierobežošanas, izskaušanas, atjaunošanas un pēckopšanas posms. Analizē atšķirības un līdzības starp NIST 800-61 un ISO 27035,	kritiski novērtē un uzlabo NIST un ISO 27035 ieviešanas efektivitāti atbilstoši jaunākajām kiberdrošības tendencēm un risku ainai.

			Izprot, ka standartos piedāvātās vadlīnijas palīdz strukturēt organizācijas incidentu pārvaldības procesu, bet vēl nevar patstāvīgi veikt padziļinātu ieviešanu.	norādot, kā katrs standarts var papildināt konkrētu organizācijas vajadzību. Pielāgo standartos noteiktās prasības reālai uzņēmuma vidē, ņemot vērā pieejamos resursus un risku profilu (piem., kāda ir uzņēmuma lielums, nozare, tehnoloģiskā infrastruktūra).	
		2.2.2.Standartu un ietvaru pielāgošana specifiskas organizācijas vajadzībām.	Identificē galvenās prasības un ieteikumus no attiecīgajiem standartiem (piem., NIST, ISO), bet vēl neveic to padziļinātu analīzi. Zina pamatjēdzienus par to, kāpēc un kad organizācijai vajadzētu pielāgot standartu prasības, lai optimāli atbilstu uzņēmuma lielumam, nozarei un iekšējai struktūrai. Atpazīst jau esošos uzņēmuma procesus, kas daļēji atbilst standartu vadlīnijām.	Kritiski izvērtē organizācijas esošās procedūras, salīdzinot tās ar standartu rekomendācijām, un spēj norādīt konkrētus uzlabojumus vai izmaiņas. Patstāvīgi pielāgo standartu/ietvaru prasības, balstoties uz uzņēmuma vajadzībām un risku profilu (piem., noformulē, kā tieši ieviest noteiktas NIST/ISO sadaļas uzņēmumā). Veic nepieciešamos pasākumus, lai organizācijā radītu vienotu izpratni par pielāgoto standartu nozīmi, un rūpējas par darbinieku apmācību atbilstoši šīm izmaiņām.	Veido un ievieš kompleksu, uz standartu un ietvaru prasībām balstītu drošības pārvaldības sistēmu, kas precīzi atspoguļo organizācijas specifiskos procesus, mērķus un risku profilu. Uzrauga un regulāri pārskata pielāgoto risinājumu efektivitāti, izmantojot mērījumus un auditus, sistemātiski pilnveido to, lai risinājums būtu gatavs mainīgajiem draudu scenārijiem un uzņēmuma izaugsmei.
	2.3.Apdraudējumu, ievainojamību un riska klasifikācija.	2.3.1.Mitre Att&ck un apdraudējumu modelēšana.	Nosauc pamata jēdzienus no MITRE ATT&CK ietvara (piem., Tactics, Techniques,	Pielieto MITRE ATT&CK ietvaru, analizējot konkrētu incidentu vai draudu gadījumu, lai	Izstrādā un ievieš padziļinātu, uz MITRE ATT&CK balstītu apdraudējumu

	8% no moduļa kopējā apjoma		Procedures – TTPs) un prot tos atšķirt. Atpazīst galvenos uzbrukuma ķēdes (kill chain) posmus un vienkāršā līmenī saprot, kā tie ir ietverti MITRE ATT&CK matricā. Izmanto paraugus vai jau zināmus scenārijus, lai identificētu vispārējas apdraudējumu modelēšanas pieejas.	noteiktu uzbrukuma posmus un izmantotās tehnikas. Kritiski izvērtē dažādas apdraudējumu modelēšanas metodes (STRIDE, PASTA u.c.), spējot argumentēt, kura ir atbilstošākā konkrētai sistēmai vai organizācijai. Veido vienkāršu apdraudējumu modeli (threat model), sasaistot to ar MITRE ATT&CK, lai organizācija varētu efektīvāk identificēt un novērst iespējamos uzbrukuma vektorus.	modelēšanas procesu, kas integrējas ar organizācijas drošības operācijām, monitoringu un reaģēšanas plāniem. Veic kompleksu risku un apdraudējumu analīzi, identificējot uzbrucēju potenciālās taktikas un tehnikas, kā arī ierosinot ilgtermiņa aizsardzības uzlabojumus.
		2.3.2.Apdraudējumu klasifikācija	Atpazīst pamata apdraudējumu veidus (ļaunatūra, sociālā inženierija, DDoS, iekšējais drauds u.c.). Uzskaita vienkāršu klasifikācijas principu, piemēram, balstītu uz apdraudējuma avotu (ārējs/iekšējs) vai mērķi (konfidencialitāte, integritāte, pieejamība). Izmanto esošas klasifikācijas tabulas vai uzņēmuma iekšējo dokumentāciju, lai noteiktu apdraudējuma kategoriju.	Kritiski izvērtē esošo apdraudējumu klasifikāciju sistēmu, papildinot vai pielāgojot to organizācijas specifikai (nozare, tehnoloģiskā bāze, riska tolerance). Patstāvīgi nosaka kritērijus (piem., uzbrukuma apjoms, sarežģītība, potenciālās sekas) apdraudējumu prioritarizācijai un var pamatot izvēlēto pieeju. Analizē konkrētas drošības situācijas, sistemātiski pieskaņojot apdraudējumu klasifikāciju uzņēmuma drošības politikai un incidentu reaģēšanas stratēģijai.	Veido un uztur daudzslāņu apdraudējumu klasifikācijas struktūru, kas aptver gan tehniskos, gan biznesa un reglamentējošos aspektus (personas datu aizsardzība, atbilstība NIS vai citiem nozares standartiem). Nodrošina, ka apdraudējumu klasifikācija tiek dinamiski atjaunota, reaģējot uz jaunām uzbrukuma tendencēm, tehnoloģiskajām pārmaiņām vai

					organizācijas pārstrukturizāciju.
		2.3.3.Riska vadības principi incidentu pārvaldībā.	Atpazīst pamatprincipus, kas saista riska vadību ar incidentu pārvaldību (piem., ietekmes un iespējamības koncepts, kritisko resursu aizsardzība). Izprot (vai spēj par vienkāršākā līmenī izskaidrot) atšķirību starp preventīviem, detektīviem un korektīviem kontroles mehānismiem incidentu gaitā. Spēj piedalīties pamata risku novērtēšanas uzdevumos, sekojot dotai metodikai, bet nepiedāvā būtiskus uzlabojumus vai korekcijas.	integrē risku analīzi visā incidenta dzīves ciklā (sākot ar identifikāciju, beidzot ar pēckopšanas pasākumiem). Izmanto formālas vai pusformālas riska vadības metodes (piem., ISO 27005 pamatprincipus) un spēj pamatot, kāpēc konkrētais modelis ir piemērots uzņēmuma situācijai. Ierosina atbilstošus drošības pasākumus, pamatojot tos ar risku analīzes rezultātiem un līdzšinējo incidentu pieredzi.	Veido un uztur stratēģisku risku pārvaldības ietvaru, kurā incidentu pārvaldība ir organiski iekļauta kopējā drošības kultūrā un biznesa plānošanā. Sistemātiski izvērtē incidentu statistiku un analizē trendus, lai ilgtermiņā samazinātu kritiskāko risku ietekmi un iespējamību, vienlaikus optimizējot resursu izmantošanu. Spēj savienot uzņēmuma risku portfeli ar augstākā vadības līmeņa lēmumiem (piem., budžeta pieprasījumi, politiku veidošana), aizstāvot drošības prioritātes un nodrošinot to atbilstību normatīvo aktu prasībām.
3.Spēj: patstāvīgi veikt incidentu apstrādi (reģistrēšanu, izpēti, ietekmes novērtēšanu atbilstoši organizācijas norādījumiem). **Zina:** incidenta dzīvescikl posmus.	3.1.Kiberdrošības incidentu apstrādes dzīvescikls 10% no moduļa kopējā apjoma	3.1.1.Incidenta dzīvescikla posmi.	Nosauc galvenos incidenta dzīvescikla posmus (sagatavošanās, atklāšana, ierobežošana, izskaušana/likvidēšana, atjaunošana, mācības(lessons learned).	Pielieto incidenta dzīvescikla posmu pieeju konkrētos piemēros, spējot pastāstīt, ko tieši darīt katrā posmā (piem., kā sagatavoties un kā novērtēt atjaunošanas kvalitāti).	Veido un vada organizācijai pielāgotu incidentu pārvaldības procesu, kas integrē visus dzīvescikla posmus vienotā rīcības plānā (piem., atbilstoši NIST SP 800-61, ISO

Izprot: incidentu obligātās ziņošanas pienākumi, nosacījumus.			Izprot katra posma vispārīgo nozīmi (piem., kāpēc sagatavošanās ir svarīga). Sekmīgi atkārto (piem., no mācību materiāla) galvenos soļus, kas katrā posmā jāveic, bet vēl nespēj tos elastīgi pielāgot sarežģītiem gadījumiem.	Kritiski izvērtē, kā incidenta dzīvescikla posmi savstarpēji mijiedarbojas (piem., kā savlaicīga atklāšana samazina ietekmi uz atjaunošanas fāzi). Adaptē dzīvescikla posmus uzņēmuma iekšējam kontekstam, piedāvājot nelielus uzlabojumus vai papildu soļus atbilstoši reālajiem resursiem un riskiem.	27035 vai citiem standartiem). Analizē un pilnveido katru posmu, pamatojoties uz statistiku, auditu un nozares labāko praksi, nodrošinot nepārtrauktu procesu uzlabošanu (*continuous improvement*).
		3.1.2.Incidenta hronoloģijas uzturēšana un dokumentēšana.	Apzinās nepieciešamību uzturēt notikumu hronoloģiju (laika zīmogi, galvenie notikumi, iesaistītās puses), lai saprastu incidenta attīstību. Izmanto pamatmetodes vai rīkus (piem., izklājlapu, vienkāršu reģistru) notikumu vai darbību ierakstīšanai, sekojot dotām instrukcijām. Nosauc priekšrocības, ko dod kārtīga dokumentācija (digitālājā kriminalistikā, juridiskās atbilstības nodrošināšanā, pēckopšanas analīzē), bet vēl nespēj to padziļināti argumentēt.	Organizē detalizētu incidenta hronoloģiju, iekļaujot tehniskos datus (logu pieraksti, sistēmu laika zīmogi) un lēmumu pieņemšanas aspektus (kurš, kad un kāpēc pieņēma konkrētu lēmumu). Pielāgo izmantotos dokumentācijas rīkus un procesus, lai tie būtu atbilstoši konkrētajam incidenta tipam un uzņēmuma procedūrām (piem., izmantojot ITSM vai speciālu drošības incidentu reģistrācijas sistēmu). Demonstrē, kā rūpīga incidenta dokumentēšana tieši palīdz labākai analīzei un forensikās izmeklēšanas veikšanai, pierādot šīs pieejas	Izstrādā un uztur padziļinātu dokumentēšanas sistēmu (piem., integrētu drošības notikumu pārvaldības sistēmu ar automātiskās žurnālu analīzes rīkiem), kas garantē precīzu un savlaicīgu informācijas fiksēšanu. Nodrošina, ka incidenta hronoloģija tiek uzturēta saskaņā ar labāko praksi un nozares normatīvajām prasībām (GDPR, valsts regulējumi), kā arī spēj pierādīt dokumentācijas integritāti un autentiskumu.

				nozīmīgumu vadībai vai kolēģiem.	
	3.2.Incidentu izpētes metodes. 10% no moduļa kopējā apjoma	3.2.1.SIEM platformas.	Zina SIEM (Security Information and Event Management) platformas pamatfunkcijas (reāllaika brīdinājumi, korelācija, notikumu uzglabāšana). Lieto SIEM platformu pamata režīmā, piemēram, atvērt notikumu sarakstu, atrast konkrētu drošības incidentu, veidot vienkāršus pārskatus. Atpazīst biežākās SIEM platformas (Splunk, IBM QRadar, Elastic Security u.c.).	Konfigurē SIEM noteikumus un veido korelācijas scenārijus, lai efektīvāk atklātu uzbrukumus vai aizdomīgas aktivitātes. Analizē SIEM ziņojumus un integrē tos ar citiem avotiem (IDS/IPS, EDR, Active Directory notikumi) vienota skatījuma veidošanai. Pielāgo SIEM platformu uzņēmuma specifiskajām prasībām (piem., atskaišu veidošana vadībai), spējot optimizēt tās darbību un izmaksas.	Veido un uztur centralizētu drošības datu ekosistēmu, kur SIEM ir viens no kodolkomponentiem un ir integrēts ar citiem drošības rīkiem (SOAR, threat intelligence platformām). Attīsta automatizāciju (skripti, orķestrācija) incidentu apstrādē, izmantojot SIEM notikumu datus un proaktīvi testējot noteikumus.
		3.2.2.Žurnālu analīzes rīki.	Pārzina pamatjēdzienus par žurnālu datu struktūru (laiks, IP adrese, process, notikuma statuss) un lietderību incidentu izpētē. Lieto vienkāršus rīkus vai iebūvētās funkcijas (grep, Windows Event Viewer) logu filtrēšanai un pamatinformācijas izvilkšanai. Atpazīst biežāk izplatītos žurnālu formātus (Windows, Linux, aplikāciju žurnāli.	Kombinē vairākus rīkus vai skriptus, lai veiktu padziļinātu žurnālu analīzi (piem., Syslog, Logstash, Kibana), strukturējot un vizualizējot datus. Analizē tendences un anomālijas, kas redzamas žurnālu datos, spējot identificēt iespējamos ielaušanās mēģinājumus vai nepilnības konfigurācijā. Izprot žurnālu standardizācijas (CEF, JSON, Common Log Format) priekšrocības un ierosina tās izmantot, lai	Veido visaptverošu logu pārvaldības stratēģiju, kas nosaka, kādus datus vākt, kā tie jāglabā, cik ilgi un kā tie jāaizsargā. Integrē logu analīzi reāllaika drošības pārraudzības un incidentu reaģēšanas procesos, izmantojot kompleksus meklēšanas vaicājumus, mašīnmācīšanos vai anomāliju detektēšanu.

				uzlabotu analīzes efektivitāti.	Projektē uzlabotas monitoringa shēmas un ieteic jaunus rīkus/žurnālu formātus, lai ilgtermiņā samazinātu pārraudzības izmaksas un palielinātu drošības notikumu atklāšanas ātrumu.
		3.2.3.Tīkla analīzes rīki.	Nosauc populārus tīkla analīzes rīkus (Wireshark, TCPDump, Zeek/Bro) un to pamatfunkcijas (paketes satura skatīšana, statistikas apkopošana). Izmanto bāzes filtrus vai vaicājumus, lai diagnosticētu vienkāršas problēmas (piem., anomāla IP adrese, neatbilstoša trafika plūsma). Apzinās tīkla protokolu pamatus (TCP/UDP, DNS, HTTP).	Kritiski analizē tīkla datplūsmu, lai noteiktu ļaunprātīgas aktivitātes pazīmes (botnet komunikācija, skenēšanas, exfiltration u.c.). Pielāgo rīku konfigurāciju (skripti, noteikumi, brīdinājumi), lai automātiski identificētu aizdomīgas datu plūsmas, atbilstoši uzņēmuma drošības politikai. Izprot sarežģītākus protokolus un tipiskas ievainojamības (piem., TLS, SSH, VPN tuneļu analīze) un demonstrē spēju tās atpazīt datu paraugos.	Izstrādā un uztur proaktīvu tīkla monitoringa pieeju, apvienojot uzvedības analīzi, signatūru atpazīšanu un reāllaika brīdinājumus (*intrusion detection*/ *prevention* sistēmas). Veic padziļinātu anomāliju un uzbrukuma vektoru izpēti, izmantojot plašu rīku un metožu spektru (mazliet pārveidotie protokoli, slēpti datu pārsūtīšanas kanāli).
		3.2.4.Digitālās izmeklēšanas (forensics) rīki.	Atpazīst galvenos digitālās izmeklēšanas soļus (pierādījumu saglabāšana, klonēšana, "hash" kalkulācija, ķēdes (*chain of custody*) uzturēšana).	Organizē pilnvērtīgu digitālās kriminalistikas analīzi, ievērojot pareizas pierādījumu iegūšanas un uzglabāšanas principus, tostarp dokumentējot procesu.	Ievieš padziļinātu digitālās forensikas metodoloģiju organizācijā, iekļaujot specifiskas procedūras dažādiem vides veidiem

			Prot izmantot vienkāršus, plaši pieejamus rīkus (piem., FTK *Imager, Autopsy, Sysinternals*) elementārai cietā diska vai atmiņas analīzei. Nosauc būtiskākos riskus, ja digitālās izmeklēšanas procesi netiek ievēroti (pierādījumu sabojāšana, juridiskās sekas), bet ne vienmēr spēj to praktiski novērst.	Spēj konfigurēt un pielāgot rīkus (*EnCase*, X-*Ways, Magnet* AXIOM) konkrētiem scenārijiem (piem., atmiņas analīzei, diskimage analīzei vai tīkla forensikai). Analizē savāktos pierādījumus, sasaistot tos ar incidenta cēloni, norādot iespējamo uzbrucēju darbību pēdas (TTPs).	(mākoņdatošana, mobilās ierīces, IoT).
	3.3.Incidentu izolēšanas un ierobežošanas metodes. 10% no moduļa kopējā apjoma	3.3.1.Ierobežošana, izolēšana un likvidēšana.	Zina atšķirību starp incidenta ierobežošanu (containment), izolēšanu (isolation) un likvidēšanu (eradication), spējot īsi raksturot katra soļa galveno mērķi. Sekmīgi atkārto organizācijas pamatinstrukcijas, kā rīkoties, lai ierobežotu incidentu (piemēram, pārtraukt aizdomīgu procesu vai atslēgt sistēmu no tīkla), bet vēl nespēj piedāvāt radošus risinājumus sarežģītām situācijām. Izprot vispārīgus drošības pasākumus, kas jāveic pirms likvidēšanas (datu rezerves kopijas, nepieciešamās	Patstāvīgi pielieto ierobežošanas un izolēšanas procedūras, spējot adaptēt tās konkrētam incidenta tipam (piemēram, izplatīta ļaunatūra vai mērķtiecīgs uzbrukums). Veic padziļinātu analīzi, vai un kad likvidēšana jāveic uzreiz, vai nepieciešams pagaidīt papildu pierādījumu vākšanu forensikas vajadzībām (riska un ieguvumu novērtējums). Kritiski izvērtē esošos procesus un ierosina konkrētus uzlabojumus (piem., skriptus, automatizāciju) incidentu ātrākai ierobežošanai un likvidēšanai.	Vada kompleksu incidentu izolēšanas un likvidēšanas stratēģiju izstrādi un ieviešanu, saskaņojot to ar organizācijas biznesa darbību un risku vadības politiku. Izstrādā elastīgus scenāriju plānus (playbooks), kas aptver dažādus uzbrukuma vektorus (endpoint, tīkla, lietojumprogrammu), lai komanda varētu reaģēt efektīvi un koordinēti. Veic incidentu plaša mēroga revīziju un analīzi (post-incident review), iekļaujot jaunas atziņas organizācijas drošības politikās un

			forensikas aktivitātes), bet ne vienmēr spēj tās pilnībā īstenot patstāvīgi.		procedūrās, lai ilgtermiņā mazinātu uzbrukumu atkārtošanās risku.
		3.3.2.Tīkla segmentācija un piekļuves kontrole.	Saprot galveno principu, kāpēc tiek lietota tīkla segmentācija (draudu izplatības mazināšana, svarīgāko resursu aizsardzība). Atpazīst vienkāršākās segmentācijas formas (piem., DMZ zona starp publisko un iekšējo tīklu, VLAN izmantošana), spēj īsumā pastāstīt, kā tās darbojas. Zina pamata piekļuves kontroles metodes (ugunsmūra noteikumi, ACL uz maršrutētāja vai slēdža), bet vēl nevar tās plaši pielāgot uzņēmuma drošības stratēģijai.	Patstāvīgi izstrādā tīkla segmentācijas risinājumu, ņemot vērā konkrētu sistēmu vai projektu drošības prasības (piem., sadalot ražošanas vidi no biroja vides). Konfigurē piekļuves kontroles noteikumus un procedūras (ugunsmūris, NAC, VPN politika), lai ierobežotu neautorizētu lietotāju vai sistēmu piekļuvi kritiskajām zonām. Regulāri pārskata un uzlabo segmentācijas un piekļuves kontroles shēmu, balstoties uz incidentu analīzi un jaunākajām draudu tendencēm.	Projektē un ievieš visaptverošu, uz riskiem balstītu segmentācijas koncepciju (*Zero Trust,* mikrosegmentācija) lielos vai sarežģītos tīklos, kur nepieciešama izcila elastība un drošības granularitāte. Integrē segmentācijas un piekļuves kontroli ar citiem drošības risinājumiem (SIEM, SOAR), nodrošinot reāllaika pielāgošanos draudu kontekstam (*dynamic policy enforcement*).
		3.3.3.Gala iekārtu un resursu izolēšana.	Atpazīst tipiskos veidus, kā var izolēt inficētu vai potenciāli bīstamu galiekārtu (fiziska atslēgšana no tīkla, speciāls "karantīnas" VLAN). Prot lietot pamata EDR (*Endpoint Detection and Response*) risinājuma funkcijas, lai atslēgtu vai ierobežotu aizdomīgas ierīces darbību.	Plāno un realizē precīzu gala iekārtu izolēšanu, mazinot iespēju, ka incidenta loks paplašinās vai ietekmē citu sistēmu darbību. Konfigurē automatizētus noteikumus drošības rīkos (EDR, MDM – *Mobile Device Management*), kas proaktīvi ierobežo gala iekārtu piekļuvi, ja tiek	Projektē centralizētu gala iekārtu pārvaldības un izolēšanas sistēmu (*Endpoint Security un Zero Trust* risinājumos), kas dinamiski maina piekļuves līmeni atkarībā no iekārtas stāvokļa un risku indikācijām.

			Ievēro bāzes drošības pasākumus, piemēram, notikumu žurnāla saglabāšanu vai lietotāju brīdināšanu, pirms gala iekārtas atvienošanas, bet vēl neizstrādā procesus kompleksi.	konstatēta ļaunprātīga darbība. Izstrādā procedūras, kā atgriezt izolēto iekārtu ražošanas vidē pēc tam, kad tas ir droši, iekļaujot verifikācijas soļus (skanēšana, ielāpi, atkārtota konfigurācija).	Uztur nepārtrauktu uzraudzību un analīzi (behavior-based detection), lai nodrošinātu proaktīvu izolēšanas mehānismu, kas ievērojami samazina izplatītu uzbrukumu ietekmi uz organizācijas tīklu.
	3.4.Ietekmes novērtēšanas metodes. 10% no moduļa kopējā apjoma	3.4.1.Ietekmes pamatjēdzieni	Spēj definēt galvenos ietekmes jēdzienus (konfidencialitāte, integritāte, pieejamība, reputācija, finansiālās sekas). Apzinās, kāpēc ietekmes novērtēšana ir svarīga uzņēmuma drošības pārvaldībā (resursu plānošanā, riska analīzē, incidentu radīto seku noteikšanā). Atpazīst vienkāršus piemērus, kur incidenta ietekme izpaužas konkrētā jomā (piem., reputācijas ietekme pēc datu noplūdes, finansiālie zaudējumi izspiedējvīrusa gadījumā).	Analizē starpību starp tiešo un netiešo ietekmi (piem., tiešās izmaksas vs. ilgtermiņa reputācijas zudums), kā arī kritiski izvērtē, kā tie savstarpēji mijiedarbojas. Pielieto ietekmes jēdzienus reālos scenārijos, piemēram, incidenta novērtēšanā, lai pamatotu prioritātes un resursu sadali (IT, finanšu, juridiskie aspekti). Skaidro, kā ietekmes pamatjēdzieni sasaistās ar organizācijas stratēģiskajiem mērķiem (piem., klientu uzticības noturēšanu, kritisko pakalpojumu nepārtrauktību).	Konsolidē ietekmes pamatjēdzienus vienotā, organizācijai pielāgotā modelī, kas palīdz veikt koordinētu un visaptverošu incidentu ietekmes analīzi. Skaidro, kā atsevišķi ietekmes faktori atspoguļojas uz biznesa ilgtspēju un konkurētspēju. Veicina drošības kultūru organizācijā, apmācot dažādus darbinieku līmeņus, lai tie izprot un spēj identificēt iespējamo ietekmi no notikumiem vai ievainojamībām.
		3.4.2.Ietekmes veidi	Spēj nosaukt galvenās kategorijas: finansiālā ietekme, reputācijas ietekme, operacionālā/tehniskā ietekme,	Klasificē ietekmes veidus konkrētā incidentā, mēģinot noteikt to savstarpējo svarīgumu (prioritāti) un iespējamo domino efektu (piem.,	Veido un uztur daudzdimensionālu ietekmes novērtēšanas pieeju, vienlaikus ņemot vērā finansiālos,

			juridiskā/atbilstības ietekme. Atpazīst katras kategorijas pamatrādītājus (piem., finansiālā – tiešās izmaksas, reputācijas – klientu uzticības zudums, operacionālā – pakalpojuma pārtraukums). Skaidro vienkāršā līmenī, kā uzbrukumi dažādi ietekmē uzņēmuma procesus (piem., DDoS – pieejamību, datu zādzība – konfidencialitāti).	reputācijas zudums var novest pie finansiāliem zaudējumiem). Izmanto piemērotus mērījumus (KPI vai KRI) katram ietekmes veidam, integrējot tos risku analīzē un sekojot tiem laika gaitā. Kritiski izvērtē, kurš ietekmes veids ir dominējošais noteiktā scenārijā un kā tas var mainīt uzņēmuma resursu ieguldījumus drošības pasākumos.	reputācijas, tehniskos un atbilstības aspektus. Integrē ietekmes veidu analīzi uzņēmuma lēmumu pieņemšanas procesos (budžeta plānošana, stratēģiskā attīstība), lai drošības aspekti tiktu pilnvērtīgi pārstāvēti.
		3.4.3.Metodoloģijas un ietvari ietekmes novērtēšanai.	Zina biežākās ietekmes novērtēšanas pieejas un ietvarus (piem., CVSS daļējais pielietojums ietekmes kontekstā, NIST risku vadības ietvars, vienkārša riska matrica). Nosauc plusus un mīnusus vispārīgām metodoloģijām (kvantitatīva vs. kvalitatīva pieeja), bet nezina, kā tās padziļināti integrēt uzņēmuma procesos. Seko dotai metodikai (piem., viegla riska matrica) un aprēķināt aptuveno ietekmes	Patstāvīgi izvēlas piemērotu ietvaru vai metodoloģiju (FAIR, NIST SP 800-30/800-37, ISO 27005) un pielāgo to incidenta kontekstam (uzņēmuma nozarei, lielumam, draudu ainai). Integrē ietekmes novērtēšanu ar citiem procesiem (incidentu reaģēšanu, forensiku, risku pārvaldību), lai nodrošinātu visaptverošu pieeju drošības pārvaldībā. Analizē metodoloģijas rezultātus un rekomendē konkrētus uzlabojumus, kas stiprinātu uzņēmuma	Izstrādā un ievieš uzlabotu, uzņēmuma specifikai pielāgotu metodoloģisko ietvaru ietekmes novērtēšanai, kur iestrādāti kvantitatīvi un kvalitatīvi rādītāji. Audita un nepārtrauktas pilnveides ceļā regulāri pārvērtē un uzlabo esošo pieeju, balstoties uz incidentu statistiku, jauniem draudiem un biznesa pārmaiņām.

			līmeni, ja scenārijs nav pārāk sarežģīts.	drošību vai mazinātu ietekmi turpmāk.	
	3.5.Komunikācija un sadarbība. 8% no moduļa kopējā apjoma	3.5.1.Iekšējā komunikācija.	Zina pamata komunikācijas ķēdi (kurš, kurā brīdī, kam un kāpēc ziņo incidentu) atbilstoši organizācijas noteikumiem. Atpazīst lomas un atbildības incidentu pārvaldības komandā (piem., IT drošības speciālists, atbildīgais vadītājs, juridiskais birojs) un saprot nepieciešamību savlaicīgi apmainīties ar informāciju. Izmanto norādītus rīkus vai kanālus (e-pasts, tērzēšanas platforma, ITSM sistēma), lai informētu kolēģus par incidenta statusu, bet ne vienmēr analizē komunikācijas efektivitāti.	Veido skaidru iekšējās komunikācijas plānu, nosakot konkrētus eskalācijas posmus un kritiskos ziņojumu punktus (piem., kad informēt valdes līmeni). Spēj koordinēt informācijas apmaiņu starp dažādām nodaļām (IT, HR, juristi, pārdošana), lai nodrošinātu vienotu izpratni par incidentu un saskaņotu rīcību. Analizē esošos iekšējās komunikācijas kanālus un piedāvā uzlabojumus (rīku integrācija, operatīvā čata istabas, droša failu koplietošana), balstoties uz incidentu pieredzi.	Integrē iekšējo komunikāciju ar plašāku drošības pārvaldības sistēmu, nodrošinot, ka incidentu ziņošana notiek automātiski un tiek vienoti dokumentēta (SIEM/ITSM/Notifikāciju platformas). Izstrādā un uztur visaptverošu iekšējās komunikācijas politiku un procesus, kas ietver arī regulārus treniņus un simulācijas, lai palielinātu darbinieku gatavību reaģēt uz incidentiem. Veicina organizācijas pārmaiņas, veidojot drošības kultūru, kurā darbinieki ir motivēti laicīgi ziņot par aizdomīgiem notikumiem, un izmanto strukturētu pieeju atgriezeniskās saites apkopošanai.
		3.5.2.Ārējā komunikācija.	Nosauc galvenās ārējās puses, kuras vajadzētu informēt par incidentu (klienti, partneri, piegādātāji, regulatoras iestādes), ja tas ir nepieciešams.	Plāno ārējās komunikācijas soļus incidenta laikā, iekļaujot detalizētu rīcības algoritmu – kam, kad un kādā formā ziņot (prese,	Plāno ārējās komunikācijas soļus incidenta laikā, iekļaujot detalizētu rīcības algoritmu – kam, kad un kādā formā ziņot (prese,

			Atpazīst vienkāršos gadījumus, kad informācijas sniegšana ārpus organizācijas ir obligāta (piem., GDPR datu aizsardzības pārkāpumi) vai ieteicama (situācijās, kas skar kritisku infrastruktūru). Spēj sniegt pamatinformāciju ārējiem interesentiem (īsa situācijas atskaite), sekojot dotam paraugam vai skriptam.	sociālie tīkli, klientu paziņojumi). Kritiski izvērtē ārējās komunikācijas riskus (konfidencialitāte, reputācijas kaitējums, juridiskie aspekti) un spēj sabalansēt atklātības un drošības intereses. Sadarbojas ar uzņēmuma vadību un citiem departamentiem, lai nodrošinātu pārdomātu un saskaņotu vēstījumu publiskajā telpā, īpaši nopietnu incidentu gadījumā.	sociālie tīkli, klientu paziņojumi). Kritiski izvērtē ārējās komunikācijas riskus (konfidencialitāte, reputācijas kaitējums, juridiskie aspekti) un spēj sabalansēt atklātības un drošības intereses. Sadarbojas ar uzņēmuma vadību un citiem departamentiem, lai nodrošinātu pārdomātu un saskaņotu vēstījumu publiskajā telpā, īpaši nopietnu incidentu gadījumā.
		3.5.3. Krīzes komunikācijas plāns.	Spēj definēt, kas ir krīzes komunikācijas plāns (struktūrēts rīcības plāns, lai samazinātu incidenta negatīvo ietekmi un novērstu paniku). Atpazīst svarīgos elementus krīzes komunikācijas plānā (kontaktpersonu saraksts, eskalācijas soļi, iepriekš sagatavoti paziņojumi), bet ne vienmēr tos patstāvīgi izstrādā. Ievēro organizācijas vispārīgās vadlīnijas krīzes situācijās (piem., izmantojot iekšējo	Izstrādā krīzes komunikācijas plānu, kurā ietverti galvenie ziņojumu scenāriji un saziņas kanāli, nodrošinot, ka plāns ir lietojams reālos gadījumos. Demonstrē, kā krīzes komunikācijas plāns integrējas ar incidentu reaģēšanas plānu un kopējo drošības stratēģiju. Testē krīzes komunikācijas plānu (tabletop vingrinājumi, simulācijas), gūstot pieredzi un uzlabojot procedūras balstoties uz reālām mācībām.	Piedalās plašas krīzes komunikācijas situācijāss, nodrošinot vienotu informatīvo telpu uzņēmuma iekšienē un ārpus tā. Integrē krīzes komunikācijas plānu vispārējās biznesa nepārtrauktības un atjaunošanas stratēģijās (BCP/DRP), lai incidenta seku novēršana noritētu pēc iespējas koordinēti un efektīvi. Adaptē krīzes komunikācijas plānu,

			rokasgrāmatu vai skriptus), bez dziļākas pielāgošanas.		ņemot vērā jaunas tendences (piem., sociālo mediju ietekmi, starptautisku mērogu), un dalās ar pieredzi nozarē, lai veicinātu labākās prakses izplatību.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited
4. "Applied Incident Response", Steve Anson, Wiley, 2020., 464.lpp
5. Carey, Marcus J. Tribe of hackers blue team: Blue team defensive advice from the biggest names in cybersecurity / Marcus J. Carey, Jennifer Jin. - 1st edition. - Indianapolis: Wiley, 2020. - xvi, 346.lpp
6. Colby, Clark. Cybersecurity incident management: masters guide / Clark Colby ; illustred by Colby Clark, Ireland Clark. - Wroclaw : Independently Published, 2020. – 666.lpp
7. Kaplan, Michael. Incident investigations and response: textbook / Michael Kaplan, Scott Scheidt. - Savannah : Amazon Digital Services LLC - Kdp Print Us, 2021. – 268.lpp
8. Colby, Clark. Cybersecurity incident management: masters guide / Clark Colby ; illustred by Colby Clark, Ireland Clark. - Wroclaw : Independently Published, 2020. – 510.lpp
9. "Mastering Cyber Incident Management", K.Hermans, Independently published, 2023, 79.lpp
10. Incident Response Techniques for Ransomware Attacks: Understand modern ransomware attacks and build an incident response strategy to work through them 1st Edition, O.Skulkin, Packt Publishing, 2022., 228.lpp

MODUĻA Informācijas sistēmu drošības inženierija, informācijas sistēmu stiprināšana, konfigurācijas uzturēšana APRAKSTS

Moduļa mērķis	Nostiprināt un pilnveidot izglītojamo prasmes veikt drošības stiprināšanu (hardening), dāžādām IKT, IS komponentēm.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.patstāvīgi apzināt, apkopot un analizēt organizācijas kiberdrošības inženierijas prasības. 2. konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos. 3. sagatavot un novērtēt organizācijas kiberdrošības risinājuma konfigurācijas atbilstību, identificēt iespējamos uzlabojumus.
Moduļa ieejas nosacījumi	Apgūti A moduļi, B daļas modulis "Incidentu klasifikācija, reaģēšana, analīze, novēršana"
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie prezentē divus dažādus stiprināšanas un konfigurācijas pārbaudes novērtējuma rezultātus (informācijas sistēmas komponentēm).
Moduļa nozīme un vieta kartē	Modulis "Informācijas sistēmu drošības inženierija, informācijas sistēmu stiprināšana, konfigurācijas uzturēšana " ir B daļas modulis, ko izglītojamie apgūst vienlaicīgi ar B daļas moduļiem IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana I " un"Kiberdrošības incidentu izmeklēšana I".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Informācijas sistēmu drošības inženierija, informācijas sistēmu stiprināšana, konfigurācijas uzturēšana SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.**Spēj:** patstāvīgi apzināt, apkopot un analizēt organizācijas kiberdrošības inženierijas prasības. **Zina:**dažādas ar kiberdrošību saistītas vispārīgās teorijas, konceptus, mērķus un prasības. Drošas programmatūras izstrādes dzīvesciklu (SDLC). Informācijas sistēmu uzbūvi, komponentes. **Izprot:** drošas informācijas sistēmas darbības principus, kiberdrošības parametru, mērījumu, veiktspējas rādījumu nozīmi konfigurācijas pārvaldībā.	8% no moduļa kopējā apjoma	1.1.Drošības stiprināšanas pamatnostādnes un apsvērumi.	Raksturo un klasificēt dažus stiprināšanas veidus.	Sttrukturēti raksturo stiprināšanas apsvērumu, veidus.	Strukturēti raksturo, atbilstoši klasificē un izskaidro priekšrocības un trūkumus stiprināšanas veidiem.
	12% no moduļa kopējā apjoma	1.2.Sistēmas pakalpojumi, grupas politiku, drošības ielāpu pārvaldība.	Pārzina grupas politiku un sistēmas pakalpojumu lomas, saprot ielāpu nepieciešamību un riskus.	konfigurēt un pārvalda grupu politikas drošībai, praktiski veic atjauninājumu pārvaldību	Izstrādā un uztur grupu drošības politikas, izplata atjaunojumus IKT infrastruktūrā, veido stratēģijas to automatizācijai.
	20% no moduļa kopējā apjoma	1.3.Servera, DB, DNS, DHCP un tīkla drošības stiprināšana	Pārzina un izprot nodrošināšanas (Servera, DB, tīkla, DNS, DHCP) atšķirības	Konfigurē un pielāgo drošības iestatījumus, implementē drošības mehānismus.	Veido un auditē drošības stiprināšanas procedūras, izstrādā un uztur drošu IKT infrastruktūru.
2.**Spēj:** konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos.	10% no moduļa kopējā apjoma	2.1.Autentifikācija, autorizācija un atsekošana (*accountability*) risinājumi	Raksturo atšķirības dažādiem autentifikācijas un autorizācijas risinājumiem	Ievieš risinājumus, identitātes, piekļuves pārvaldības un multifaktoru autentifikācijai	Pielāgo un veic izmaiņas, atbilstoši organizācijas vajadzībām.

Zina:drošas programmatūras izstrādes dzīvesciklu (SDLC). Informācijas sistēmu uzbūvi, komponentes. Drošības arhitektūras principus. Konfigurācijas parametru nosacījumus. Kriptogrāfijas pamatprincipus. **Izprot:**drošas informācijas sistēmas darbības principus. Drošības bāzes līnijas (Security baseline) pielietojumu. Konfigurācijas pārvaldības procedūras. Autentifikācijas un autorizācijas nozīmi.	20% no moduļa kopējā apjoma	2.2. Kriptogrāfijas pamatprincipi: Jaukšanas un sālīšanas metodes; kriptogrāfijas algoritmi un noslēpumi;šifrēts e-pasts, šifrētais sakaru protokols (SSL, TLS) Simetriskā šifrēšana, Asimetriskā šifrēšana, Kriptogrāfijas mehānisma projektēšanas, uzbūves un konfigurācijas ievainojamību testi			Izmanto, pielāgo, konfigurē kriptogrāfiskos risinājumus datu aizsardzībai.
3.**Spēj:** sagatavot un novērtēt organizācijas kiberdrošības risinājuma konfigurācijas atbilstību, identificēt iespējamos uzlabojumus. **Zina:**kiberdrošības risinājuma tehniskās prasības. Dažādas sociālās inženierijas un krāpniecības metodes. Kiberhigiēnas pamatprincipus. **Izprot: i**nformācijas sistēmu stiprināšanas(hardening) pasākumus.	10% no moduļa kopējā apjoma	3.1. Programmatūras izstrādes dzīvescikls kiberdrošībā: a)ievades validācijas, autentifikācijas un autorizācijas nozīme, b)drošu un nedrošu kodēšanas prakse.	Raksta vienkāršu kodu ar minimālu drošības izpratni. Izprot drošas kodēšanas principus, bet nepiemēro tos konsekventi.	Ievieš drošas kodēšanas praksi, ievērojot OWASP vadlīnijas un integrē drošības rīkus (SAST/DAST), prezentēt rezultātus.	Var kodā noteikt un pamanīt nedrošas sesijas apstrādes, nepareizas API konfigurācijas, kriptogrāfijas nepilnības un piedāvāt labojumus.
	20% no moduļa kopējā apjoma	3.2. Drošības stiprināšanas analīzes rīku apskats.	Pārzina drošības stiprināšanas, konfigurācijas analīzes rīkus	Praktiski pielieto rīkus konfigurācijas analīzei	Veiksmīgi pielāgo iestatījumus, ņemot vērā anlīzē konstatētās neatbilstības.

Konfigurācijas failu izveides un analīzes nosacījumus.					

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmi IKT sistēmu drošības testēšanā, atklāto ievainojamību ietekmes uz testējamo sistēmu novērtēšanā un piedāvāt iespējamos risinājumus ievainojamību novēršanā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. iepazīties ar noteiktiem kiberdrošības testu uzdevumiem, apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes. 2. apzināt testa plānu un piemērot drošības testēšanas metodes un rīkus, lai noteiktu iespējamos kiberuzbrukuma vektorus. 3. izstrādāt un veikt sistemātiskus dažāda līmeņa kiberdrošības prasību novērtējumus pēc iepriekš definētiem kritērijiem (izprot atšķirības starp //tai skaitā - vulnerability scan, penTest, health checks).
Moduļa ieejas nosacījumi	Apgūti B daļas moduļi " IKT un kiberdošības normatīvo aktu piemērošana", "Incidentu klasifikācija, reaģēšana, analīze, novēršana", "IS drošības inženierija, IS stiprināšana, konfigurācijas uzturēšana".
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudes darbu- praktisko darbu par sistēmas drošības testēšanu.
Moduļa nozīme un vieta kartē	Modulis " IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana I " ir B daļas modulis.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA IKT drošības testēšana, ievainojamību atklāšana, novērtēšana, novēršana SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1**. Spēj:** iepazīties ar noteiktiem kiberdrošības testu uzdevumiem; apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes. **Zina:** drošības testēšanas standarti un ietvari; metodes un rīki, kas atbalsta prasību apkopošanu un lēmumu pieņemšanas analīzi. **Izprot:** dažādas drošības testēšanas metodikas (piem. OWASP).	1.1.Drošības testēšanas pamati. 10% no moduļa kopējā apjoma	1.1.1. Drošības testēšanas nozīme un mērķis.	Izskaidro drošības testēšanas nozīmi IT sistēmu aizsardzībā, nosauc galvenos drošības testēšanas mērķus (piemēram, drošības ievainojamību identificēšana un novēršana).	Skaidri formulē drošības testēšanas mērķus, pielāgojot tos konkrētiem projektam vai organizācijai.	Analizē reālus drošības apdraudējumu piemērus un sasaistīt tos ar drošības testēšanas nozīmi, definē drošības testēšanas stratēģiju un tās mērķus konkrētā kontekstā, pamatojoties uz riska analīzi.
		1.1.2. Drošības testēšanas plānošana*. Black box, gray box, white box testing*.	Izskaidro atšķirības starp *black box, gray box un white box* testēšanas pieejām.	Iesaka drošības testēšanas plānu, pamatojot konkrētas pieejas piemērotību dažādos testēšanas scenārijos.	Detalizēti izstrādā drošības testēšanas plānu, pamatojoties uz konkrētās sistēmas prasībām un riskiem. Argumentē un pielāgo testēšanas stratēģiju atbilstoši sistēmas apdraudējumu analīzei, nodrošinot efektīvu resursu izmantošanu.
		1.1.3. Drošības testēšanas loma un nozīme sistēmas izstrādes un uzturēšanas ciklā.	Uzskaita galvenās darbības, kas nepieciešamas drošības testēšanas plānošanā. Izskaidro, kurās sistēmas izstrādes un uzturēšanas posmos tiek veikta drošības testēšana	Identificē un izskaidro drošības testēšanas ietekmi uz sistēmas izstrādes un uzturēšanas efektivitāti un kvalitāti.	Piedāvā un pamato ieteikumus par drošības testēšanas iekļaušanu dažādos sistēmas izstrādes posmos.
	1.2.IKT komponentes.	1.2.1. IKT komponentes un to loma IS.	Uzskaita galvenās IKT komponentes (piemēram, aparatūra,	Detalizēti izskaidro katras IKT komponentes funkcijas IS darbībā,	Analizē dažādu IKT komponenšu nozīmi

	5% no moduļa kopējā apjoma		programmatūra, tīkli, datubāzes) un izskaidro to lomu IS darbībā.	sniedzot piemērus no reālām situācijām. Izskaidro, kā konkrēta komponenta nepareiza darbība var ietekmēt IS veiktspēju vai drošību.	konkrētā IS kontekstā un novērtē to efektivitāti. Piedāvā uzlabojumus IS arhitektūrā, ņemot vērā komponentu spējas un ierobežojumus.
		1.2.2. IKT komponenšu savstarpējā mijiedarība.	Izskaidro kā IKT komponentes sadarbojas, lai nodrošinātu IS darbību. Skaidro vienkāršus piemērus, kā dažādas komponentes mijiedarbojas (piemēram, serveris, tīkla infr. ierīces un lietotāja ierīces).	Detalizēti apraksta galvenos mijiedarbības procesus starp IKT komponentēm (piemēram, datu plūsmas, savienojumi, protokoli).	Izprot mijiedarbības nepilnību ietekmi uz drošības un veiktspējas problēmām.
		1.2.3. Testēšanas ietekme uz sistēmas un datu pieejamību un integritāti, datu konfidencialitāti.	Skaidro testēšanas veidu ietekmi uz sistēmas darbību, ietekmes pieejamību, integritāti un datu konfidencialitāti.	Izskaidro dažādu testēšanas metožu ietekmi uz sistēmas un datu pieejamību, integritāti un konfidencialitāti.	Identificē riskus, kas saistīti ar testēšanas procesu, un piedāvāt risinājumus to mazināšanai.
	1.3.Testēšanas metodoloģijas. 10% no moduļa kopējā apjoma	1.3.1.Testēšanas metodoloģijas un to nozīme.	Skaidro galvenās drošības testēšanas metodoloģijas un to atšķirības.	Raksturo dažādas testēšanas metodoloģijas, izvēlas atbilstošāko atkarībā no drošības testēšanas mērķa un tvēruma.	Analizē drošības testēšanas metodoloģiju priekšrocības un trūkumus dažādos kontekstos un stratēģiski kombinē tās, lai panāktu maksimālu efektivitāti.
		1.3.2.Testēšanas sagatavošanās un izpildes posmi.	Nosauc un raksturo drošības testēšanas galvenos posmus.	Detalizēti apraksta un organizē katru testēšanas posmu.	Izprot sagatavošanās posma ietekmi uz testēšanas precizitāti un efektivitāti, veic pielāgojumus testēšanas posmos atkarībā no nepieciešamības un situācijas.
2.**Spēj:** apzināt testa plānu un piemērot drošības testēšanas	2.1.Manuālās drošības	1.1. Manuālās drošības testēšanas	Izskaidro manuālās drošības testēšanas lomu kā specifisku un	Izskaidro saikni starp manuālo drošības testēšana un	Patstāvīgi izveido vienkāršu manuālās testēšanas plānu, ņemot

metodes un rīkus, lai noteiktu iespējamos kiberuzbrukuma vektorus. **Zina:** testēšanas ietekmes apzināšana uz testējamajām IKT komponentēm; zināmo ievainojamību avotus (piem. CVE, CERT.LV publicētie u.c.), testēšanas standartus un vadlīnijas. **Izprot:** dažādu IS ievainojamības (avotus, vektorus, tipoloģijas).	testēšanas metodes. 10% no moduļa kopējā apjoma	nozīme un scenāriji, kurā to izmanto.	padziļinātu pieeju ievainojamību noteikšanai, ko automatizētie rīki var nepamanīt. Skaidro vienkāršus scenārijus izmantošanai, piemēram, autentifikācijas sistēmu testēšana vai datu ievades validācija.	automatizēto testēšanu, īpaši sarežģītu ievainojamību un loģikas kļūdu identificēšanai. Identificē specifiskus scenārijus, kuros manuāla testēšana ir būtiska, piemēram, piekļuves kontroles analīzē vai lietotāju darbību simulācijās. Izmantot manuālo testēšanu, lai identificētu ievainojamības, kas balstītas uz uzņēmuma specifiskām sistēmas implementācijām.	vērā sistēmas specifiku un ievainojamību identificēšanas prioritātes. Novērtē un pamato, kuras ievainojamības ir jātestē manuāli un kur nepieciešama papildināšana ar automatizāciju. Patstāvīgi dokumentē un argumentē, kā manuālā testēšana papildina automatizēto pieeju konkrētajā sistēmā.
		1.2. Manuāla ievainojamību identificēšana un ekspluatēšana.	Identificē pamata ievainojamības, piemēram, vājas paroles, atvērtus portus vai ievades validācijas trūkumus, izmantojot manuālas metodes. Izskaidro, kā ievainojamību ekspluatēšana tiek veikta, piemēram, simulējot SQLi vai XSS. Raksturo vienkāršus rīkus vai metodes ievainojamību manuālai pārbaudei.	Sistemātiski analizē ievainojamību, izmantojot tādas pieejas kā ievades manipulācija, autentifikācijas problēmu pārbaude un piekļuves kontroles testēšana. Veic pamata ievainojamību ekspluatāciju, izmantojot tādus rīkus kā Burp Suite manuālā režīmā vai pielāgotus skriptus. Izskaidro, kā dokumentēt atrastās ievainojamības un novērtēt to ietekmi uz sistēmu.	Patstāvīgi veic mērķtiecīgus testus, izmantojot manuālas pieejas, lai pārbaudītu ievainojamības, kuras automatizētie rīki neidentificē (piemēram, biznesa loģikas kļūdas, piekļuves kontroles problēmas). Patstāvīgi veic vienkāršu ievainojamības ekspluatāciju, izmantojot Burp Suite, Postman vai skriptus, lai pierādītu ievainojamības praktisko ietekmi. Argumentē un dokumentē ekspluatācijas rezultātus, sasaistot tos ar riska līmeņa novērtējumu.

	2.2.Automatizētās testēšanas metodes un rīki. 10% no moduļa kopējā apjoma	2.1. Automatizētās drošības testēšanas nozīme un scenāriji, kurā to izmanto.	Izprot automatizētās testēšanas iespējas salīdzinājumā ar manuālo testēšanu. Izprot automatizētās testēšanas pielietojumu (to izmanto regulārām pārbaudēm, lielu sistēmu skenēšanai vai atkārtotu problēmu identificēšanai). Izskaidro piemērus, kur izmanto automatizāciju, piemēram, tīmekļa lietotņu vai tīkla infrastruktūras testēšanā.	Analizē un pielāgo automatizētās testēšanas rīkus konkrētām vajadzībām, piemēram, regulārai ievainojamību pārbaudei vai ievainojamību skenēšanai pirms produkcijas ieviešanas. Izskaidro automatizācijas priekšrocības lielāku sistēmu vai sarežģītu tīkla arhitektūru testēšanā. Izmanto dažādus rīkus, lai identificētu vairākas ievainojamības vienlaikus un izvērtēt rezultātus.	Patstāvīgi konfigurēt un pielāgo automatizētās testēšanas rīkus, piemēram, OWASP ZAP, lai precīzi pārbaudītu ievainojamības konkrētā sistēmā. Patstāvīgi izveido automatizētas testēšanas skriptus vai sekvences, lai veiktu regulāras pārbaudes un integrēt tos CI/CD procesā. Kritiski analizē automatizācijas rezultātus un pieņem lēmumu par manuālas testēšanas nepieciešamību, pamatojoties uz rezultātiem.
		2.2. Tīmekļa aplikāciju ievainojamību skenēšanas rīki.	Skaidro pamata rīkus, piemēram, OWASP ZAP, Burp Suite un Nikto, un to izmantošanas mērķus. Paskaidro, kā šie rīki palīdz identificēt ievainojamības, piemēram, SQL injekcijas, XSS vai nepareizas piekļuves kontroles. Veic pamata skenēšanu ar rīku un analizēt iegūtos rezultātus.	Izmanto rīkus, piemēram, OWASP ZAP vai *Burp Suite,* lai izveidotu pielāgotus ievainojamību skenēšanas scenārijus. Analizē iegūtos skenēšanas rezultātus un prioritizē konstatētās problēmas. Paskaidro darbības ierobežojumus un prot tos kombinēt ar manuālu testēšanu.	Patstāvīgi pielāgo tīmekļa lietotņu skenerus (piemēram, *Burp Suite*, OWASP ZAP) konkrētām drošības pārbaudēm, piemēram, autentifikācijas mehānismu pārbaudei vai sesijas pārvaldībai. Pamato, kā kombinēt vairāku rīku sniegtos rezultātus, lai iegūtu visaptverošu ievainojamību analīzi. Patstāvīgi veido ieteikumus, balstoties uz skenēšanas rezultātiem, iekļaujot to kritiskuma novērtējumu un prioritātes.

		2.3. Datu pārraides tīklu un infrastruktūras skenēšanas rīki.	Izskaidro rīku kā *Nmap, Wireshark* un OpenVAS galvenās funkcijas tīkla un infrastruktūras skenēšanā. Izskaidro, kā šie rīki tiek izmantoti, lai identificētu atvērtus portus, nepareizus konfigurējumus vai citus tīkla drošības trūkumus. Veic vienkāršu tīkla skenēšanu, izmantojot Nmap, un izprot pamatrezultātus.	Veic padziļinātu tīkla un infrastruktūras analīzi, izmantojot *Nmap,* OpenVAS un citus rīkus, lai identificētu riskus, piemēram, novecojušus protokolus vai vājas konfigurācijas. Izskaidro dažādu tīkla skenēšanas režīmu (piemēram, TCP SYN scan vai UDP scan) priekšrocības un pielietojumus. Izmanto iegūtos rezultātus, lai izstrādātu ieteikumus tīkla uzlabošanai.	Izmanto *Nmap* un *Wireshark*, lai detalizēti analizētu tīkla ievainojamības, piemēram, novecojušus protokolus vai atvērtus portus. Patstāvīgi veic infrastruktūras ievainojamību skenēšanu ar rīkiem, piemēram, OpenVAS, pielāgojot skenēšanas parametrus specifiskām vajadzībām. Pamato, kā izmantot tīkla skenēšanas rezultātus, lai izveidotu riska novērtējumu un ieteiktu uzlabojumus.
		2.4. Dažādu rīku/skriptu izvēle un pielāgošana atbilstoši situācijai.	Izprot rīku un skriptu izvēles piemērotību konkrētam uzdevumam vai scenārijam. Raksturo populārākos rīkus un izvēlas atbilstošu pamata drošības testēšanai. Veic vienkāršas pielāgošanas skriptu vai konfigurāciju konkrētai drošības pārbaudei.	Izvēlas rīkus, kas vislabāk atbilst konkrētajai drošības testēšanas situācijai, un pielāgo to iestatījumus vai skriptus specifiskām prasībām. Izmanto skriptu valodas, piemēram, Python vai Bash, lai automatizētu specifiskus testēšanas procesus. Kombinē vairākus rīkus un skriptus vienotā testēšanas procesā.	Patstāvīgi izvēlas optimālo rīku vai skriptu, ņemot vērā testēšanas uzdevumu un sistēmas īpatnības. Patstāvīgi modificē un pielāgo vienkāršus skriptus (piemēram, Python vai Bash), lai efektīvāk veiktu automatizētus testus konkrētai ievainojamībai. Pamato, kā integrēt vairākus rīkus vienotā testēšanas procesā, nodrošinot efektivitāti un atkārtojamību.
	2.3.Dažādu sistēmu populārās ievainojamības	2.3.1. Populārākās tīmekļa ievainojamības un atbilstošās CVE.	Skaidro galvenās ievainojamības, piemēram, SQL injekcijas, XSS un CSRF, un to	Identificē un detalizēti izskaidro galvenās tīmekļa ievainojamības,	Identificē specifiskas ievainojamības, piemēram, IDOR, SQL injekcijas vai XSS, un

	un to ekspluatēšana. (CVE) 10% no moduļa kopējā apjoma		iespējamo ietekmi uz sistēmu. Identificē piemērus no CVE datu bāzes, kas attiecas uz šīm ievainojamībām.	piemēram, SQL injekcijas, XSS, CSRF un IDOR. Izmanto CVE datu bāzes konkrētu ievainojamību analīzei un risinājumu plānošanai. Sasaista ievainojamības ar atbilstošajiem CVE piemēriem un to risinājumiem.	sasaista tās ar atbilstošajiem CVE identifikatoriem. Argumentēti izskaidro identificēto ievainojamību ietekmi uz sistēmas drošību un veic ekspluatāciju, lai to demonstrētu. Pamato, kā ieteikt remediāciju risinājumus, balstoties uz CVE analīzi.
		2.3.2. Populārākās OS ievainojamības un atbilstošās CVE.	Raksturo populāro OS ievainojamību nepietiekamu piekļuves kontroli, novecojušas programmatūras vai vājas noklusējuma konfigurācijas. Paskaidro, kā CVE datu bāze sniedz informāciju par ievainojamībām un to risinājumiem.	Identificē izplatītās OS ievainojamības, piemēram, privilege escalation, remote code execution, un analizēt to ietekmi. Izmanto CVE datu bāzi, lai noteiktu risinājumus un aizsardzības stratēģijas. Sagatavo ieteikumus OS drošības uzlabošanai, pamatojoties uz konstatētajām ievainojamībām.	Patstāvīgi analizē OS ievainojamības, piemēram, privilege escalation vai remote code execution, un dokumentēt to ietekmi uz sistēmu. Atrod atbilstošos CVE identificētajiem riskiem un izmantot šos datus aizsardzības plānošanai. Patstāvīgi simulē vienkāršu ekspluatāciju, lai demonstrētu ievainojamības efektu.
		2.3.3. Datu pārraides tīklu protokolu ievainojamības un atbilstošās CVE.	Izprot TCP, DNS un ARP protokolu specifiskas ievainojamības, piemēram, TCP SYN flood, DNS spoofing vai ARP poisoning. Paskaidro, kā CVE datu bāze var palīdzēt noteikt un novērst šīs ievainojamības.	Identificē un izskaidro datu pārraides tīklu ievainojamības, piemēram, DNS spoofing, ARP poisoning, un TCP SYN flood. Izmanto CVE informāciju, lai analizētu protokolu drošības trūkumus un risinājumus. Izskaidro, kā šīs ievainojamības ietekmē tīkla darbību un drošību.	Patstāvīgi identificē specifiskas tīkla protokolu ievainojamības, piemēram, TCP reset attacks vai ARP poisoning, un sasaistīt tās ar CVE. Veic protokolu ievainojamību analīzi, izmantojot Wireshark vai citus tīkla analīzes rīkus. Patstāvīgi izveido ieteikumus tīkla aizsardzības uzlabošanai,

					balstoties uz identificētajām ievainojamībām.
	2.4.Datu pārraides tīklu un infrastruktūras drošības testēšana. 10% no moduļa kopējā apjoma	2.4.1. Datu pārraides tīklu un infrastruktūras nozīme kopējā IS drošības kontekstā.	Izskaidro tīkla drošības nozīmīgumu, lai aizsargātu informācijas sistēmu no apdraudējumiem. Izprot neaizsargātās infrastruktūra drošības riskus.	Detalizēti izskaidro, kā tīklu un infrastruktūras drošība ietekmē IS aizsardzību pret ārējiem un iekšējiem draudiem. Identificē vājās vietas tīkla arhitektūrā un ierosināt uzlabojumus.	Patstāvīgi analizē tīkla infrastruktūru un norāda uz potenciāliem drošības draudiem, piemēram, vājām konfigurācijām vai neaizsargātiem savienojumiem. Patstāvīgi iesaka praktiskus uzlabojumus tīkla drošības stratēģijai.
		2.4.2. OSI modelis un tā analīze drošības testēšanas kontekstā.	Skaidro OSI modeļa pamata slāņus un to lomu datu pārraides procesā. Izskaidro, kā katrs slānis var būt potenciāls uzbrukumu mērķis un ir jātestē attiecīgi.	Analizē katru OSI modeļa slāni drošības kontekstā un identificē potenciālās ievainojamības. Izskaidro konkrētu OSI slāņu aizsardzību pret apdraudējumiem, piemēram, datu šifrēšanas vai autentifikācijas problēmām.	Patstāvīgi analizē katru OSI slāni, identificē drošības ievainojamības un ierosināt konkrētus risinājumus, piemēram, šifrēšanu vai autentifikāciju. Pamato, kā OSI slāņi mijiedarbojas un kā šīs mijiedarbības var radīt drošības riskus.
		2.4.3. Tīkla resursu atklāšana (*enumeration*) un izmantotie rīki.	Izprot enumeration nozīmi tīkla resursu un lietotāju identificēšanai. Skaidro tādus rīkus kā Netcat, Nmap vai Enum4linux, un to pamatfunkcijas.	Izmanto tādus rīkus kā Netcat, Nmap, Enum4linux, lai identificētu tīkla resursus un konfigurācijas problēmas. Raksturo enumeration lomu padziļinātā tīkla analīzē un draudu identificēšanā.	Patstāvīgi veic padziļinātu tīkla resursu analīzi, izmantojot Enum4linux, Netcat vai Nmap. Patstāvīgi dokumentē atklātos tīkla resursus un to iespējamo izmantošanu uzbrukumos.
		2.4.4. Tīkla piekļuves kontroles un vāju autentifikācijas metožu pārbaudes metodes.	Izprot vājo paroļu un nepietiekamo autentifikācijas metožu radītos drošības riskus. Skaidro pamata metodes, piemēram, vārdnīcas	Izmanto metodes, piemēram, password cracking vai vārdnīcas uzbrukumus, lai identificētu	Patstāvīgi testē piekļuves kontroles sistēmas un autentifikācijas mehānismus, izmantojot simulētus uzbrukumus, piemēram, vārdnīcas

			uzbrukumus, un pielieto tās.	autentifikācijas nepilnības. Testē piekļuves kontroles sistēmu efektivitāti, simulējot dažādus piekļuves mēģinājumus.	uzbrukumus vai brute-force. Izstrādā ieteikumus autentifikācijas stiprināšanai.
		2.4.5 Atvērtu portu un pakalpojumu analīze. Testēšana pret CVE uz atvērto portu servisiem.	Izskaidro atvērtu portu analīzes nozīmi ievainojamību identifikācijā. Izmanto rīkus, piemēram, Nmap, lai identificētu atvērtus portus un pakalpojumus.	Izmanto Nmap un līdzīgus rīkus, lai identificētu atvērtus portus un to ievainojamības. Izmanto CVE informāciju, lai analizētu atvērtu portu servisu riskus un novērstu ievainojamības.	Patstāvīgi analizē atvērtus portus un izmantot CVE datu bāzi, lai identificētu potenciālās ievainojamības. Pamato, kā izmantot Nmap un Metasploit, lai simulētu testēšanu pret atvērto portu servisiem.
		2.4.6. Tīkla protokolu ievainojamības (TCP, DNS, ARP)	Skaidro galvenās protokolu ievainojamības, piemēram, DNS cache poisoning vai ARP spoofing. Izprot, kā šīs ievainojamības var apdraudēt tīkla drošību.	Identificē un analizē ievainojamības, piemēram, TCP reset attacks, DNS cache poisoning, un ARP spoofing. Izskaidro, kā šīs ievainojamības var tikt izmantotas tīkla apdraudēšanai un kā tās novērst.	Patstāvīgi identificē un analizē protokolu ievainojamības, kā arī veic pamata ekspluatāciju, lai demonstrētu risku. Patstāvīgi piedāvā risinājumus šo ievainojamību novēršanai.
		2.4.7. IDS/IPS u.c. drošības sistēmu apiešana/ efektivitātes testēšana.	Izprot IDS/IPS lomu draudu atklāšanā un novēršanā. Izskaidro metodes, lai identificētu, vai IDS/IPS reaģē uz potenciālajiem uzbrukumiem.	Veic pamata testus, lai novērtētu IDS/IPS spēju atklāt dažādus draudus, piemēram, ļaunprātīgu datu pārraidi. Raksturo drošības sistēmu stiprās un vājās puses un ierosina uzlabojumus.	Patstāvīgi veic testus, lai noteiktu IDS/IPS sistēmu efektivitāti, un dokumentēt ieteikumus to uzlabošanai. Simulē ļaunprātīgus uzbrukumus, lai novērtētu IDS/IPS reaģēšanas spēju.
		2.4.8. Wi-Fi tīklu testēšana.	Izskaidro, ka Wi-Fi tīklu testēšanā tiek pārbaudīta autentifikācija, šifrēšana un tīkla konfigurācija.	Testē Wi-Fi tīklu drošību, analizējot autentifikāciju, šifrēšanu un konfigurācijas ievainojamības.	Patstāvīgi veic Wi-Fi tīkla drošības testēšanu, izmantojot Aircrack-ng, Kismet, lai identificētu

			Skaidro pamata rīkus, piemēram, Aircrack-ng, un to izmantošanas mērķus.	Izmanto rīkus, piemēram, Aircrack-ng, lai pārbaudītu WPA/WPA2 drošību.	vājas konfigurācijas vai šifrēšanas trūkumus. Pamato, kā izstrādāt ieteikumus drošības uzlabošanai, pamatojoties uz testēšanas rezultātiem.
	2.5.Sociālās inženierijas izmantošana testēšanā. 10% no moduļa kopējā apjoma	2.5.1. Cilvēku psiholoģija un sociālās inženierijas nozīme testēšanā.	Izskaidro, kā sociālā inženierija balstās uz cilvēku psiholoģijas izmantošanu, lai iegūtu sensitīvu informāciju. Skaidro cilvēku darbības kā drošības ķēdes vājāko posmu.	Raksturo sociālās inženierijas lomu, izmantojot cilvēka kļūdas vai psiholoģiskus trūkumus. Identificē situācijas, kurās sociālā inženierija var būt veiksmīga, piemēram, phishing uzbrukumi.	Patstāvīgi izveido vienkāršu sociālās inženierijas scenāriju, lai identificētu drošības trūkumus, kas saistīti ar cilvēka uzvedību. Pamato cilvēka psiholoģijas nozīmi drošības kontekstā un ierosina preventīvus pasākumus.
		2.5.2. Sociālās inženierijas metodes un to pielietojuma situācijas.	5.2. Raksturo pamata metodes, piemēram, phishing, pretexting vai baiting. Skaidro doto metožu pielietojumu, lai piekļūtu sistēmām vai datiem, apejot tehniskās aizsardzības.	5.2. Izmanto pamata sociālās inženierijas metodes, piemēram, phishing, pretexting vai tailgating, reālos simulācijas scenārijos. Izskaidro, kā šīs metodes tiek izmantotas, lai piekļūtu konfidenciālai informācijai vai sistēmām.	5.2. Patstāvīgi veic simulētus sociālās inženierijas uzbrukumus, piemēram, phishing vai pretexting, un analizēt to efektivitāti. Patstāvīgi iesaka pasākumus organizācijas darbinieku apmācībai un sociālās inženierijas risku mazināšanai.
3.Spēj: izstrādāt un veikt sistemātiskus dažāda līmeņa kiberdrošības prasību novērtējumus pēc iepriekš definētiem kritērijiem (izprot atšķirības starp //tai skaitā - vulnerability scan, penTest, health checks). **Zina:** objektīva novērtējuma veikšanas	3.1. Testēšanas rezultātu dokumentācija un analīze. 10% no moduļa kopējā apjoma	3.1.1. Testēšanas rezultātu dokumentēšanas labā prakse.	Izprot strukturētas un skaidras testēšanas rezultātu dokumentācijas nepieciešamību. Pieraksta konstatētās ievainojamības, norādot galvenos parametrus: ievainojamības nosaukumu, atrašanās vietu un konstatēšanas datumu.	Izveido strukturētus un viegli saprotamus testēšanas rezultātus, izmantojot piemērotas dokumentācijas platformas. Izprot, kā izmantot standartizētus formātus, iekļaujot šādus parametrus: ievainojamības nosaukumu, aprakstu,	Patstāvīgi izveido detalizētas un profesionālas testēšanas dokumentācijas sistēmu, kas ietver ievainojamību identificēšanu, analīzi un risinājumu ieteikumus. Pielāgo un pamato dokumentācijas saturu dažādām auditorijām (tehniskai komandai,

paņēmieni, rīki, matricas; Zināmo ievainojamību avoti (piem. CVE, CERT.LV publicētie u.c.). Testēšanas standarti un vadlīnijas. **Izprot:** dažādus drošības testēšanas rīkus un risinājumus.			Izmanto standarta formātu, piemēram, tabulas vai vienkāršotas atskaites struktūru.	ietekmi, klasifikāciju, ekspluatācijas iespējamību un ieteikumu tās novēršanai. Izseko atrisinātās un neatrisinātās ievainojamības, uzturot aktuālu informāciju.	vadībai, ārējiem partneriem). Pamato, kā izmantot standartus, piemēram, OWASP Testing Guide, lai nodrošinātu dokumentācijas atbilstību nozares labākajām praksēm.
		3.1.2. Testēšanas rezultātu klasificēšana un strukturēšana	Izskaidro testēšanas rezultātu klasifikāciju pēc kategorijām, piemēram, sistēmas komponentēm (lietojumprogrammas, tīkla elementi). Piešķir katrai ievainojamībai nozīmīguma līmeni, piemēram, augsts, vidējs vai zems. Izmanto pamata klasifikācijas rīkus vai metodes, lai strukturētu ievainojamības.	Klasificē ievainojamības pēc to ietekmes, prioritātes un riska līmeņa, piemērojot tādas metodes kā CVSS (Common Vulnerability Scoring System). Strukturē rezultātus pa kategorijām (tīkla ievainojamības, lietotņu ievainojamības, fiziskā drošība) un analizēt katras kategorijas kopējo ietekmi uz sistēmu. Izprot klasifikāciju rīku nozīmi, lai palīdzētu uzņēmumam pieņemt lēmumus par resursu sadali ievainojamību novēršanai.	Patstāvīgi izmanto uzlabotus rīkus un metodoloģijas, piemēram, CVSS un MITRE ATT&CK, lai klasificētu un strukturētu ievainojamības pēc ietekmes, riska un ekspluatācijas iespējamības. Patstāvīgi izveido pielāgotas klasifikācijas kategorijas, kas atbilst konkrētās organizācijas biznesa mērķiem un prioritātēm. Patstāvīgi identificē korelāciju starp dažādām ievainojamībām un nosaka kopējos drošības trūkumus.
		3.1.3. Testēšanas atskaites/pārskata veidošana.	Izveido vienkāršu testēšanas pārskatu, kurā iekļauts: -īss ievads par testēšanas mērķiem, -izmantotās metodes, -galvenie rezultāti un ieteikumi. Izveido pārskatu, kas piemērots dažādiem	Veido profesionālas un detalizētas atskaites, kas piemērotas gan tehniskai, gan vadības auditorijai. Izprot, kā iekļaut atskaitē šādas sadaļas: -testēšanas mērķi, -izmantotās metodes, konstatētās	Patstāvīgi izveido visaptverošu atskaiti, kas ietver ievainojamību analīzi, riska novērtējumu un detalizētus ieteikumus to novēršanai, tostarp konkrētus tehniskus soļus. Argumentēti izmanto vizuālus rīkus (grafikus,

			mērķauditorijas līmeņiem (tehniskiem un netehniskiem lasītājiem).	ievainojamības (strukturēti), -to risinājumu ieteikumi un secinājumi. Prezentē atskaites galvenos punktus saprotami un pārliecinoši.	diagrammas), lai uzskatāmi demonstrētu rezultātus un prioritātes. Skaidro un pamato, kā prezentēt pārskatus dažādām ieinteresētajām pusēm, nodrošinot, ka informācija ir skaidra un darbībai piemērota.
	3.2.Atklāto ievainojamību kritiskuma novērtējums. 10% no moduļa kopējā apjoma	3.2.1. Ievainojamību klasifikācija (ietekme uz IS darbību, biznesa ietekme, ekspluatēšanas sarežģītība)	Izskaidro ievainojamības klasifikācijas kategorijas pēc ietekmes uz informācijas sistēmas darbību, biznesa operācijām un ekspluatācijas sarežģītības. Identificē vienkāršas klasifikācijas kategorijas, piemēram: -Ietekme uz IS darbību: kritiska, būtiska, minimāla. -Biznesa ietekme: augsta, vidēja, zema. -Ekspluatēšanas sarežģītība: viegli, vidēji, sarežģīti.	Novērtē ievainojamību ietekmi, ņemot vērā trīs aspektus: ietekmi uz IS darbību (kritiska, būtiska, minimāla), biznesa ietekmi (finansiāls zaudējums, reputācijas risks) un ekspluatācijas sarežģītību (vienkārša, vidēja, sarežģīta). Izmanto klasifikāciju, lai palīdzētu organizācijai efektīvi reaģēt uz ievainojamībām. Pamato rīku un metožu ietekmi uz klasifikācijas procesu automatizāciju.	2.1.Patstāvīgi izmanto CVSS kombinācijā ar biznesa prioritātēm, lai klasificētu ievainojamības pēc to ietekmes uz sistēmu un organizāciju. Pamato, kā apvienot tehnisko un biznesa ietekmi, lai identificētu kritiskās ievainojamības. Patstāvīgi izstrādā pielāgotas klasifikācijas sistēmas organizācijām ar specifiskām drošības prasībām.
		3.2.2. Ievainojamību radīto risku novērtēšana un ietekmes scenāriju izstrāde.	Izprot ievainojamības radītā riska konceptu un nosaka risku vienkāršos terminos (augsts, vidējs, zems). Apraksta vienkāršus ietekmes scenārijus(piemēram, ja ievainojamība tiek ekspluatēta, kāds būs potenciālais kaitējums?)	Novērtē riskus, izmantojot kvantitatīvas un kvalitatīvas pieejas, piemēram, CVSS vai organizācijas iekšējos kritērijus. Izveido vienkāršus scenārijus, kas ilustrē potenciālo ievainojamības izmantošanas ietekmi, piemēram, datu noplūdi	Patstāvīgi izstrādā detalizētus riska scenārijus, kuros iekļauts potenciālo ievainojamības ekspluatācijas ceļš, iespējams kaitējums un novēršanas stratēģijas. Pamato, kā veikt padziļinātu riska analīzi, izmantojot tādas metodes kā Threat Modeling un Impact Mapping.

			Pamato, kuri elementi vai dati var tikt apdraudēti ievainojamības rezultātā.	vai sistēmas darbības traucējumus. Pamato, kā ieteikt preventīvos pasākumus, balstoties uz riska novērtējumu.	Patstāvīgi novērtē gan tiešo, gan netiešo ievainojamības ietekmi uz biznesa procesiem.
	3.3.Atklāto ievainojamību novēršanas ieteikumi. 5% no moduļa kopējā apjoma	3.3.1. Ievainojamību novēršanas prioritizēšana**.**	Izprot, ka ievainojamības jānovērš, prioritizējot pēc to kritiskuma (augsta ietekme un viegla ekspluatēšana tiek risinātas pirmās). Veic vienkāršu ievainojamību prioritizāciju, izmantojot klasifikācijas rīkus vai manuāli.	Novērtē, kuras ievainojamības ir jānoved līdz risinājumam vispirms, pamatojoties uz to riska līmeni un ekspluatācijas iespējamību. Pamato, kā izmantot tādas pieejas kā Pareto princips vai CVSS, lai noteiktu prioritātes. Izstrādā vienkāršu ievainojamību novēršanas plānu, iekļaujot prioritātes un termiņus.	Patstāvīgi izstrādā prioritizēšanas modeli, kurā apvienoti tehniskie un biznesa faktori, piemēram, ievainojamības ekspluatācijas iespējamība un tās ietekme uz uzņēmuma darbību. Pamato, kā efektīvi plānot resursus un termiņus, lai novērstu kritiskās ievainojamības vispirms. Patstāvīgi iesaka stratēģiskus uzlabojumus organizācijas pieejai ievainojamību novēršanai.
		3.3.2. Programmatūras ievainojamību novēršana.	Izprot nepieciešamību pēc regulāriem programmatūras atjauninājumiem, lai novērstu ievainojamības. Iesaka vienkāršus risinājumus, piemēram, lietot programmatūras ielāpus vai pārbaudīt ievades datus, lai izvairītos no injekcijas uzbrukumiem.	Identificē un iesaka piemērotus programmatūras atjauninājumus, ielāpus vai kodu labošanas pieejas. Pamato, kā ieteikt drošas programmēšanas prakses, piemēram, ievades sanitizāciju, lai novērstu tādas ievainojamības kā SQL injekcijas vai XSS. Komunicē ar izstrādātājiem, lai nodrošinātu ievainojamību efektīvu novēršanu.	Patstāvīgi identificē un iesaka drošas programmēšanas un kodēšanas prakses, lai mazinātu ievainojamību risku jau sistēmas izstrādes laikā. Argumentēti novērtē un pielieto pieejamos atjauninājumus un ielāpus, nodrošinot to ātru un drošu ieviešanu. Pamato, kā integrēt drošības testēšanu izstrādes procesos, piemēram, izmantojot DevSecOps principus.

		3.3.3. Tīkla un infrastruktūras ievainojamību novēršana.	Identificē pamata tīkla drošības problēmas, piemēram, neaizsargātus portus vai vājas paroles. Izprot, ka ievainojamību novēršanai jāveic noteikti pasākumi, piemēram, aizvērt nevajadzīgus portus, konfigurēt ugunsmūrus vai stiprināt piekļuves kontroles.	Identificē un iesaka risinājumus, piemēram, portu slēgšanu, drošu konfigurāciju pielietošanu, ugunsmūru stiprināšanu vai tīkla segmentēšanu. Pamato, kā veikt novēršanas pasākumus, piemēram, SSL/TLS šifrēšanas ieviešanu vai neizmantoto pakalpojumu atspējošanu. Sadarbojas ar infrastruktūras administratoriem, lai nodrošinātu risinājumu īstenošanu.	Patstāvīgi iesaka un palīdz ieviest risinājumus, kas stiprina tīkla drošību, piemēram, tīkla segmentēšanu, ugunsmūru konfigurāciju un drošības monitoringu. Patstāvīgi izmanto NIST Cybersecurity Framework vai līdzīgas vadlīnijas, lai strukturētu tīkla drošības stratēģiju. Pamato, kā plānot un veikt regulāras pārbaudes, lai identificētu un novērstu jaunas tīkla ievainojamības.
		3.3.4. Tīmekļa programmu ievainojamību novēršana.	Izprot, ka XSS un SQL injekciju novēršanai nepieciešama datu validācija un sanitizācija. Iesaka vienkāršus risinājumus, piemēram, drošas ievades pārbaudes ieviešanu un HTTP drošības galveņu izmantošanu.	Iesaka un palīdz ieviest risinājumus ievainojamību, piemēram, CSRF, IDOR vai nepareizu autentifikāciju, novēršanai. Pamato drošības rīku (piemēram, Content Security Policy, WAF) pielietojumu, lai mazinātu riskus tīmekļa lietotnēs. Iesaka labākās prakses, piemēram, sesiju vadību vai drošu paroļu glabāšanu.	Patstāvīgi piedāvā un ievieš konkrētus risinājumus tīmekļa ievainojamību novēršanai, piemēram, Content Security Policy, rate limiting vai drošu autentifikācijas un autorizācijas mehānismu ieviešanu. Pamato, kā pielietot OWASP Application Security Verification Standard (ASVS), lai izvērtētu un uzlabotu tīmekļa lietotņu drošību. Profesionāli sadarbojas ar izstrādātājiem, lai veicinātu drošu kodēšanu un testēšanu.
		3.3.5. Fiziskās drošības un cilvēciskā faktora	Izprot piekļuves kontroles (piemēram, drošas paroles un piekļuves	Izskaidro efektīvu risinājumu fiziskās drošības stiprināšanai	Patstāvīgi identificē un novērš fiziskās drošības vājās vietas, piemēram,

		ievainojamību novēršana/mazināšana.	žurnāli) nozīmi fiziskās drošības risku samazināšanā. Iesaka darbinieku apmācību un procedūras, lai samazinātu cilvēciskā faktora radītās ievainojamības, piemēram, izvairīties no sociālās inženierijas upuriem.	nepieciešamību, piemēram, piekļuves karšu izmantošanu vai video uzraudzību. Izstrādā ieteikumus darbinieku apmācībai, lai mazinātu sociālās inženierijas riskus. Pamato, kā apvienot tehniskos un cilvēciskos pasākumus, lai panāktu kopējo drošības uzlabošanu.	piekļuves kontroles sistēmu uzlabošanu vai fizisko aizsardzību svarīgajām sistēmām. Argumentēti iesaka un palīdz ieviest organizācijas mēroga darbinieku apmācību programmas, kas vērstas uz sociālās inženierijas risku mazināšanu. Pamato, kā apvienot tehniskos un organizatoriskos pasākumus, lai stiprinātu kopējo aizsardzību pret fiziskajiem un cilvēciskajiem riskiem.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited
4. Mastering Active Directory: Design, Deploy, and Protect Active Directory Domain Services for Window Server 2022, 3rd Edition", Dishan Francis, Packt Publishing, 2021., 778.lpp
5. "Mastering Windows Security and Hardening: Secure and Protect Your Windows Environment from Cyber Threats Using Zero-Trust Security Principles, 2nd Edition" – Mark Dunkerley, Matt Tumbarello, Packt Publishing, 2022., 816.lpp
6. "Windows Server 2022 & PowerShell All-in-One For Dummies", Sara Perott, For Dummies, 2022., 784.lpp
7. Hickey, Matthew. Hands on Hacking / Jennifer Arcuri. - New York : John Wiley & Sons Inc, 2020. – 608. lpp
8. Khawaja, Gus. Kali linux penetration testing bible : ultimate guide to pentesting with Kali Linux / Gus Khawaja. - 1st edition. - New York : John Wiley & Sons Inc, 2021. – 512. lpp
9. Beaver, Kevin. Hacking for dummies: must-have resource for anyone who wants to keep their data safe / Kevin Beaver. - 7th edition. - New York : John Wiley & Sons Inc, 2022. – 416. lpp
10. Dombrovskis, Valērijs. KIBER ES: viss par kiberpasauli / Valērijs Dombrovskis, Luīze Berga. - Rīga: Ezerrozes grāmatas, 2021., 14.3 lpp
11. "Hacking APIs: Breaking Web Application Programming Interfaces", Corey J. Ball, No Starch Press, 2022.

MODUĻA Kiberdrošības incidentu izmeklēšana I APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmes kiberdrošības incidentu izpētē un saistītās informācijas apstrādē.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. veikt kiberdrošības incidentu izpēti (izmeklēšanu) sadarbībā ar incidentu izpētē iesaistītajām pusēm. 2. veikt ar kiberdrošības incidentu saistīto informācijas apstrādi (tai skaitā veikt IS žurnālu (auditācijas pierakstu) analīzi. 3. sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta reaģēšanā, novēršanā iesaistītajām pusēm 4. analizēt un apkopot auditācijas pierakstos identificētos notikumus pārskata ziņojumā.
Moduļa ieejas nosacījumi	Apgūti A daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudījumu, kurā ir teorētisko zināšanu pārbaudes jautājumi un praktiskā darba daļa – praktiska kiberdrošības incidentu izpēte un apstrāde pēc dotā scenārija.
Moduļa nozīme un vieta kartē	Modulis " IKT un kiberdrošības normatīvo aktu piemērošana " ir B daļas modulis. To apgūst vienlaicīgi ar A daļas moduļiem "IKT un dro’’sibas arhitektūras pamati", "Kiberdrošības un risku pārvaldības pamati".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Kiberdrošības incidentu izmeklēšana I SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.Spēj: veikt kiberdrošības incidentu izpēti (izmeklēšanu) sadarbībā ar incidentu izpētē iesaistītajām pusēm. **Zina:** incidenta dzīvesciklu (tā sastāvdaļas - priekšizpētei nepieciešamo informāciju), incidenta risināšanā iesaistīto pušu pienākumus un atbildības robežas. **Izprot:** kiberdrošības uzbrukumu metodes, avotus, vektorus, klasifikāciju.	1.1.Kiberdrošības incidentu izpēte. 20 % no moduļa kopējā apjoma	1.1.1.Kiberdrošības incidentu izmeklēšana.	Saprot pierādījumu nozīmi un nepieciešamību tos korekti apstrādāt. Veic pamata dokumentēšanu un sadarbību ar pieredzējušiem speciālistiem.	Analizē vienkāršus incidentus, izmanto digitālās izmeklēšanas rīkus. Sagatavo sākotnēju analīzi un sniedz atbalstu incidentu izmeklēšanā.	Veic incidentu izmeklēšanas procesu, nosaka uzbrukuma vektorus un ierosina atbilstošus aizsardzības pasākumus. Izstrādā drošības pārkāpumu novēršanas ieteikumus.
		1.1.2.Incidentu dzīves cikls.	Apraksta incidenta dzīves cikla posmus, saprot katra posma nozīmi.	Koordinē incidentu pārvaldības soļus. Veic sākotnēju ietekmes novērtējumu un dokumentē risināšanas gaitu.	Pārzina incidentu dzīves ciklu, ieskaitot preventīvo un pēcekspluatācijas analīzi. Optimizē incidentu pārvaldības procesus un nodrošina pastāvīgus uzlabojumus.
		1.1.3.Kiberdrošības uzbrukumu analīze.	Skaidro uzbrukumu veidus (DDoS, phishing, malware, ransomware u.c.). Saprot, kā šie uzbrukumi darbojas un kādu apdraudējumu tie rada.	Identificē uzbrukumu indikatorus un analizē iespējamos uzbrukumu vektorus. Izmanto pamata rīkus, lai pētītu aizdomīgu tīkla un sistēmas darbību.	Veic padziļinātu uzbrukumu analīzi, nosaka uzbrucēju taktikas un stratēģijas (TTPs) un sniedz rekomendācijas par efektīviem aizsardzības pasākumiem.

					Pārzina specializētus rīkus un metodoloģijas (MITRE ATT&CK u.c.).
2.Spēj: veikt ar kiberdrošības incidentu saistīto informācijas apstrādi (tai skaitā veikt IS žurnālu (auditācijas pierakstu) analīzi. Spēja sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta reaģēšanā, novēršanā iesaistītajām pusēm. **Zina**: žurnālu (auditācijas pierakstu) analīzes metodes, paņēmienus, rīkus, struktūru, avotu specifiku, sintakses nosacījumus, analīzes, korelācijas principus. **Izprot:** incidentu apstrādes un incidenta izmeklēšanas procesu atšķirības.	2.1.1.Informācijas apstrāde un analīze kiberdrošības incidentu izmeklēšanā. 20 % no moduļa kopējā apjoma	2.1.1.Kiberdrošības incidentu saistīto datu vākšana un apstrāde.	Skaidro kiberdrošības incidentu analīzei būtiskās informācijas nozīmi. Izmanto pamata rīkus un metodes datu vākšanai un sākotnējai analīzei.	Analizē savāktos datus, salīdzina dažādus avotus un nosaka aizdomīgas aktivitātes. Izmanto specializētus rīkus (SIEM, žurnālu analīzes rīkus) informācijas analīzei.	Sistemātiski apstrādā lielus datu apjomus, veic padziļinātu korelāciju starp dažādiem avotiem un izstrādā efektīvus drošības pārvaldības pasākumus pamatojoties uz analīzi.
		2.1.2.Datu korelācijas metožu izmantošana incidentu analīzē.	Apraksta datu korelācijas būtību un kā tā palīdz identificēt kiberdrošības incidentus. Izmanto vienkāršas metodes, lai salīdzinātu un analizētu datus.	Izmanto datu korelācijas rīkus (piemēram, SIEM), lai analizētu notikumus un noteiktu potenciālos draudus. Prot interpretēt korelētus datus un noteikt iespējamās uzbrukumu pazīmes.	Sasaista dažādu avotu datus, lai atklātu sarežģītus kiberdraudus.
	2.2.Incidentu apstrādes un izmeklēšanas procesu atšķirības. 10% no moduļa kopējā apjoma	2.2.1.Proaktīvā un reaktīvā incidentu pārvaldība.	Izprot atšķirību starp proaktīvo un reaktīvo pieeju incidentu pārvaldībā. Skaidro preventīvi pasākum u nozīmi incidentu risku samazināšanā.	Pārzina pamatmetodes, kā analizēt un reaģēt uz incidentiem.	Izstrādā ieteikumus uzlabojumiem proaktīvām un reaktīvām drošības stratēģijām.
		2.1.2.Pēdincidentu analīze un uzlabošanas pasākumi.	Skaidro pēdincidentu analīze nozīmīgumu. Piedalās incidentu atskaišu sagatavošanā un identificē vienkāršus uzlabojumus.	Veic padziļinātu incidenta cēloņu analīzi, piedāvā uzlabojumus, izmantojot esošos rīkus un metodes. Iesaistās pēcincidentu analīzes procesā.	Nosaka atkārtotu problēmu tendences un iesaka efektīvus preventīvos pasākumus. Iesaka organizācijas drošības politikas uzlabojumus.

	2.3.Žurnālu (auditācijas pierakstu) analīzes metodes un rīki. 30% no moduļa kopējā apjoma	2.3.1.Žurnālu analīzes struktūra un avotu specifika	Raksturo sistēmas un drošības žurnālus, to ģenerēšanu un to nozīmi kiberdrošībā.	Identificē dažādu žurnālu avotus (serveri, ugunsmūri, IDS/IPS, SIEM u.c.), izprot to struktūru un analizē ierakstus, meklējot iespējamas drošības problēmas.	Strukturēti analizē lielu datu apjomu no dažādiem žurnālu avotiem, pielietojot efektīvas meklēšanas un filtrēšanas metodes. Pielāgo un automatizē žurnālu analīzes procesus.
		2.3.2.Notikumu korelācija un analīzes rīki	Apraksta notikumu korelāciju un tās lomu drošības datu analizē. Pielieto pamata rīkus, kas atvieglo datu apstrādi un korelāciju.	Izmanto SIEM sistēmas un citus rīkus, lai veiktu notikumu korelāciju un noteiktu neparastus modeļus žurnālos. Prot analizēt dažādu avotu savstarpējo saistību.	Veido pielāgotus korelācijas noteikumus un integrē vairākus datu avotus, lai atklātu sarežģītus uzbrukumu scenārijus.
		2.3.3.Anomāliju detektēšana.	Raksturo normālu un nenormālu sistēmas uzvedību.	Izmanto dažādus rīkus un metodes (statistiskās analīzes, mašīnmācīšanās u.c.), lai noteiktu potenciālus kiberdraudus, balstoties uz anomālijām.	Pārzina progresīvas anomāliju detektēšanas metodes un to pielietojumu kiberdrošības uzraudzībā.
3.Spēj: analizēt un apkopot auditācijas pierakstos identificētos notikumus pārskata ziņojumā. **Zina:** dažādu kiberdrošības atbalsta struktūru (SOC, CERT, HelpDesk) darbības pamatprincipus, galvenās atšķirības, atbilstības prasības. **Izprot:** digitālās	3.1.Kiberdrošības incidentu analīze. 20% no moduļa kopējā apjoma	3.1.1.Auditācijas pierakstu analīze un ziņošana	Analizē auditācijas pierakstus, atpazīst aizdomīgus notikumus un sagatavo vienkāršus atskaišu ziņojumus. Izmanto analīzes rīkus, piemēram, SIEM platformas. Skaidro auditācijas pierakstu nozīmi drošības pārvaldībā. Apraksta žurnāla datus un to izmantošanu incidentu analīzē.	Analizē auditācijas pierakstus, atpazīst aizdomīgus notikumus un sagatavo vienkāršus atskaišu ziņojumus. Izmanto analīzes rīkus, piemēram, SIEM platformas.	Veic padziļinātu auditācijas pierakstu analīzi, identificē sarežģītus uzbrukumus un sagatavot detalizētus incidentu ziņojumus. Pielieto automatizētas analīzes metodes un pielāgo SIEM rīkus organizācijas vajadzībām.

izmeklēšanas atvērto rīku (OSINT u.c.) darbības ierobežojumus.		3.1.2.Kiberdrošības atbalsta struktūras un to loma	Skaidro SOC un CERT pamatfunkcijas un to nozīmi kiberdrošības incidentu pārvaldībā. Apraksta atbilstošus incidentu eskalācijas un ziņošanas procesus.	Efektīvi sadarbojas ar SOC, CERT un HelpDesk, nododod nepieciešamo informāciju par incidentiem. Ievēro procedūras un palīdz incidentu izmeklēšanas procesā, izmantojot pamata rīkus un metodes.	Sniedz detalizētu analīzi SOC un CERT komandām, palīdzot identificēt un novērtēt drošības draudus. Piedalās iekšējo procesu uzlabošanā.
		3.1.3.Digitālās izmeklēšanas rīki un ierobežojumi	Skaidro OSINT rīku nozīmi un to ierobežojumus.	Izmanto digitālās izmeklēšanas rīkus, lai iegūtu publiski pieejamu informāciju par draudiem. Ievēro juridiskās normas.	Veic padziļinātu digitālo izmeklēšanu, lai identificētu potenciālos draudus.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA Kiberdrošības risinājumi (uzstādīšana, uzturēšana, novērtēšana) I APRAKSTS

Moduļa mērķis	Sniegt zināšanas un veicināt prasmes kiberdrošības risinājumos, to uzstādīšanā, uzturēšanā un novērtēšanā.
Moduļa uzdevumi	Attīstīt izglītojamo zināšanas un prasmes: 1.apkopot un analizēt organizācijas kiberdrošības risinājumu tehniskos kritērijus, rezultatīvos rādītājus, veiktspējas metrikas; identificēt iespējamos kiberdrošības risinājumu uzlabojumus. 2. apzināt, atlasīt, grupēt dažāda veida un līmeņa tehniskās prasības (kā piemēram, kiberdrošības, funkcionālās/nefunkcionālās) prasības nepieciešamajam IKT risinājumam. 3. salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus. 4. ieviest un uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām.
Moduļa ieejas nosacījumi	Apgūti visi B daļas moduļi.
Moduļa apguves novērtēšana	Moduļa noslēgumā tiek kārtots noslēguma darbs, kas sastāv no divām daļām: 1.teorētiskā daļa, kurā izglītojamais atbild uz jautājumiem rakstiskā formātā vai elektroniski. 2.praktiskā daļa, kurā balstoties uz situācijas aprakstu izglītojamais atlasa, salīdzina un piedāvā un ievieš konkrētu kiberdrošības risinājumu, kas būtu piemērots dotajai situācijai.
Moduļa nozīme un vieta kartē	Modulis "Kiberdrošības risinājumu uzstādīšana, uzturēšana, novērtēšana 1" ir "B" daļas modulis. To apgūst vienlaicīgi ar moduļiem "Kiberdrošības incidentu izmeklēšana". Moduļa turpinājums ir C daļā "Kiberdrošības risinājumu uzstādīšana, uzturēšana, novērtēšana II".
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Kiberdrošības risinājumi (uzstādīšana, uzturēšana, novērtēšana) I SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.Spēj: apkopot un analizēt organizācijas kiberdrošības risinājumu tehniskos kritērijus, rezultatīvos rādītājus, veiktspējas metrikas; identificēt iespējamos kiberdrošības risinājumu uzlabojumus. **Zina:** Drošības sistēmu veidus, datu pārraides tīklu infrastruktūru un tās komponentes, drošas programmatūras izstrādes dzīvescikls. **Izprot:** kiberdrošības parametru, mērījumu, veiktspējas rādītāju nozīmi konfigurācijas pārvaldībā.	30% no moduļa kopējā apjoma	1.1.Organizācijas kiberdrošības risinājumu veidi.	Nosauc un apraksta organizācijas kiberdrošības risinājumu veidus (IDS, IPS, VPN, datu šifrēšana utt.) un tiem atbilstošus tehniskos kritērijus, rezultatīvos rādītājus un veiktspējas metrikas.	Raksturo kiberdrošības organizācijas risinājumu veidus un tiem atbilstošus tehniskos kritērijus, rezultatīvos rādītājus un veiktspējas metrikas.	Izvērtē kiberdrošības organizācijas risinājumu veidus un tiem atbilstošus tehniskos kritērijus, rezultatīvos rādītājus un veiktspējas metrikas. Identificē iespējamos uzlabojumus.
		1.2.Drošas programmatūras dzīvescikls.	Nosauc un apraksta drošas programmatūras izstrādes dzīvescikla etapus.	Izprot drošas programmatūras izstrādes dzīvescikla etapus.	Pielieto drošas programmatūras izstrādes dzīvescikla procesus.
		1.3.Datu pārraides tīkla infrastruktūra.	Pārzina datu pārraides tīkla infrastruktūru (topoloģijas, zonējumu) un tās komponentes (komutācijas, maršrutēšanas ierīces, serveri u.c.).	Izprot un daļēji spēj veikt datu pārraides tīklu infrastruktūru, tās komponentes un konfigurāciju.	Veic izmaiņas datu pārraides tīklu infrastruktūrā, tās komponentēs un konfigurācijā, lai uzlabotu drošību.
		1.4.Kiberdrošības risinājumu uzlabojumu ieviešana.	Izskaidro identificētos nepieciešamos uzlabojumus.	Apraksta un objektīvi pamato identificēto uzlabojumu nepieciešamību.	Izvērtē potenciālos ieguvumus no uzlabojumu ieviešanas
		1.5.Kiberdrošības parametru,	Nosauc un apraksta kiberdrošības parametrus, mērījumus,	Izskaidro kiberdrošības parametru, mērījumu,	Izvērtē kiberdrošības parametrus,

		mērījumu, veiktspējas rādītāji.	veiktspējas rādītājus (vides drošības līmeņi, paroļu drošība, konfidencialitātes, pieejamības, integritātes līmeņi utt.).	veiktspējas rādītāju nozīmi.	mērījumus, veiktspējas rādītājus.
2.Spēj: apzināt, atlasīt, grupēt dažāda veida un līmeņa tehniskās prasības (kā piemēram, kiberdrošības, funkcionālās/nefunkcionālās) prasības nepieciešamajam IKT risinājumam. **Zina:** drošības arhitektūras principus, prasību ieviešanas procedūras, konfigurācijas parametru nosacījumus. **Izprot:** Gala ierīču (angl. *end-point*) drošības nozīmi kopējā drošības arhitektūrā.	30% no moduļa kopējā apjoma	2.1.Kiberdrošības risinājumu prasības.	Identificē un grupē tehniskās un funkcionālās prasības kiberdrošības risinājumam.	Raksturo un apraksta tehniskās un funkcionālās prasības kiberdrošības risinājumam.	Izvērtē kiberdrošības risinājumu funkcionālās un tehniskās prasības.
		2.2.Drošības sistēmu arhitektūra.	Izskaidro drošības sistēmas arhitektūru (dizains, tehnoloģijas, politikas u.tml.) un gala ierīču drošības nozīmi kopējā drošības arhitektūrā.	Apraksta drošības sistēmu arhitektūru un gala ierīču nozīmi kopējā drošības arhitektūrā.	Pielieto drošības sistēmu arhitektūru organizācijas kiberdrošības veicināšanai.
		2.3.Kiberdrošības risinājumu uzstādīšanas procedūras.	Nosauc un apraksta kiberdrošības risinājumu uzstādīšanas procedūras.	Izskaidro kiberdrošības risinājumu uzstādīšanas procedūras un to konfigurācijas parametrus.	Pēc iepriekš noteiktām instrukcijām realizē kiberdrošības risinājumu uzstādīšanas procedūras un konfigurē risinājumu parametrus.
3.Spēj: salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus. **Zina:** sistēmu integrācijas metodes, savietojamības prasības, drošības bāzes līnijas (angl. *Security baseline*). **Izprot:** izmaiņu pārvaldības ietekmi	20% no moduļa kopējā apjoma	3.1.Kiberdrošības risinājumi.	Izpēta informāciju un atlasa kiberdrošības risinājumu produktus un tiem atbilstošus analogus (tirgus analīze).	Apraksta kiberdrošības risinājumu īpašības un to analogus. Veic risinājumu salīdzināšanu.	Izvērtē kiberdrošības risinājumu produktus un to analogus un izvēlas optimālāko risinājumu.
		3.2.Sistēmu integrācija un savietojamība.	Nosauc un apraksta sistēmu integrācijas metodes (piem., vertikālā un horizontālā)	Izskaidro sistēmu integrācijas metodes un savietojamības prasības.	Pielieto sistēmu integrācijas metodes un savietojamības prasības.

darbības nepārtrauktības nodrošināšanā			un savietojamības prasības.		
		3.3.Drošības bāzes līnijas.	Nosauc un apraksta drošības bāzes līnijas dažādiem risinājumiem (piem., CIS drošības bāzes līnijas).	Izskaidro drošības bāzes līnijas dažādiem risinājumiem.	Pielieto drošības bāzes līnijas dažādiem risinājumiem.
		3.4.Izmaiņu pārvaldībasdarbības nepārtrauktības nodrošināšana.	Apraksta izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.	Izskaidro izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.	Izvērtē izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.
4.Spēj: ieviest un uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām. **Zina:** izmaiņu pārvaldības principi, testēšanas veidi, metodes, rīki. **Izprot:** datu aizsardzības, kiberdrošības, izmaiņu pārvaldības risisnājumus.	20% no moduļa kopējā apjoma	4.1.Kiberdrošības risinājumi organizācijas drošības arhitektūra.	Nosauc atbilstošākos kiberdrošības risinājumus organizācijas drošības arhitektūrai.	Apraksta atbilstošāko kiberdrošības risinājumu uzturēšanas darbus pēc iepriekš noteiktām instrukcijām un tehniskās dokumentācijas.	Ievieš un uztur atbilstošākos kiberdrošības risinājumus organizācijas drošības arhitektūrā pēc iepriekš noteiktām instrukcijām un tehniskās dokumentācijas.
		4.2.Izmaiņu pārvaldes principi, metodes un rīki.	Nosauc un apraksta izmaiņu pārvaldes principus, izmaiņu testēšanas veidus, metodes un rīkus.	Izprot izmaiņu pārvaldes principus, izmaiņu testēšanas veidus, metodes un rīkus.	Pielieto izmaiņu pārvaldes principus, izmaiņu testēšanas veidus, metodes un rīkus.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA Kiberdrošības tehniķa prakse APRAKSTS

Moduļa mērķis	Pilnveidot izglītojamo spējas, prasmes un kompetences, nodrošinot teorētisko zināšanu pārnesi praktiskās aktivitātēs - kiberdrošības prasību uzturēšanā. Informācijas sistēmu (IS) drošības testēšanā, incidentu risināšanā, izmeklēšanā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības. 2. identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses. 3. apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam. 4. sagatavot kiberdrošības risinājumu rezultātu apkopojumu tālākai analīzei. 5. interpretēt no risinājumiem iegūtos (izgūtos) rezultātus. 6. precīzi izpildīt testēšanas plānu, scenārijus, izmantojot atbilstošus rīkus un metodes sistēmu ievainojamību identificēšanai.
Moduļa ieejas nosacījumi	Apgūti A, B un C daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais atbilstoši prakses programmai prezentē darba mapi (portfolio) par prakses darbavietā veiktajiem uzdevumiem, pašvērtējumu un darbavietas prakses vadītāja vērtējumu/rekomendāciju. 1.Titullapa. 2.Prakses vietas apraksts t.sk., kiberdrošības prasību apraksts. 3.Risinājumu vai procesu salīdzinošā analīze (kritēriji, riski). 4.Risinājuma vai procesa ieviešanas un uzturēšanas prasību novērtējums. Moduļa apguves pašvērtējums. Noslēguma prezentācija, kurā iekļauti secinājumi un atziņas par prakses laikā apgūto. Izglītojamais iesniedz atbilstošos profesionālās kvalifikācijas prakses dokumentus.
Moduļa nozīme un vieta kartē	Modulis "Kiberdrošības tehniķa prakse" ir programmas B daļas modulis. Modulis "Kiberdrošības tehniķa prakse" ir noslēdzošais modulis "Kiberdrošības tehniķa" profesionālās kvalifikācijas iegūšanai, paredzēts apgūto profesionālo kompetenču nostiprināšanai darba vidē.

MODUĻA Kiberdrošības tehniķa prakse SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.Spēj: patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības. **Zina:** izprot kiberdrošības stratēģiju, kiberdrošības normtīvo aktu prasības, Latvijas kiberdrošības atbildīgo institūciju hierarhiju un to uzdevumus. Autentifikācijas, autorizācijas; datu pārraides tīkla darbības prasības, kā arī IKT infrastruktūras uzbūvi. **Izprot:** Normatīvo aktu analīzes rīkus, metodes un paņēmienus, normatīvo aktu prasības un to nozīmi organizācijas kiberdrošības nodrošināšanā, informācijas sistēmu drošības standartu nosacījumus; Datu pārraides tīklu uzbūvi, darbību, tīklu drošību; drošības sistēmu, servisu veidus.	25% no moduļa kopējā apjoma	Drošības prasību analīze dažādos tvērumos: a) Nacionālās kiberdrošības likums, b) Vispārīgā datu aizsardzības regula, c) industrijas standarti, d) organizācijas kiberdrošības dokumentācijas, e) organizācijas IKT in drošības arhitektūra).	Nosaka un raksturo pamata kiberdrošības prasības, kas attiecas uz organizāciju; piedalās kiberdrošības pārbaužu veikšanā.	Analizē organizācijas kiberdrošības prasību ieviešanas līmeni. Veido organizācijas drošības dokumentācijas kontrolsarakstu, atbilstoši normatīvo aktu prasībām, standartiem, drošības arhitektūrai).	Nosaka organizācijas kiberdrošības prasību kopu atbilstoši subjekta klasifikācijai. Izlases kārtībā analizē drošības dokumentācij, ziņojumus un pārskatus. Dokumentē auditu, atbilstības pārbaudes rezultātus, atbilstoši speciālista norādījumiem.
2.Spēj: identificēt kiberdrošības incidentos,	25% no	2.1.Incidentu apstrāde	Saprot incidentu apstrādes	Veic incidentu izpēti un ietekmes novērtēšanu,	Atbilstoši kompetencei pieņem

ietekmētos resursus un iesaistītās puses. **Zina:** incidenta dzīveciklu (tā sastāvdaļas, priekšizpētei nepieciešamo informāciju) **Izprot:** incidentu apstrādes standartus, labo praksi, digitālās izmeklēšanas nozīmi, risku, draudu, ievianojamību klasifikāciju, incidentu obligātās ziņošanas pienākumus, nosacījumus.	moduļa kopējā apjoma	(reģistrēšana, izpēte, ietekmes novērtēšana, klasifikācija, atbilstoši organizācijas iekšējām kārtībām.	pamatprincipu, raksturo incidenta klasifikācijas principus.	piemērojot veidnes un vadlīnijas.	lēmumus par atbilstošām incidentu apstrādes stratēģijām, reakcijām, nodrošinot atbilstību organizācijas iekšējām kārtībām.
3.Spēj: apzināt tehniskās un funkcionālās prasības nepieciešamajam kiberdrošības risinājumam; sagatavot kiberdrošības risinājuma rezultātu apkopojumu, interpretēt rezultātus. **Zina:** Drošības sistēmu veidus. Datu pārraides tīklu infrastruktūru un tās komponentes. Drošas programmatūras izstrādes dzīvesciklu. Drošības arhitektūras principus. Prasību ieviešanas procedūras. Konfigurācijas parametru nosacījumus. Sistēmu integrācijas metodes. Savietojamības prasības. Drošības bāzes līnijas (Security baseline).	25% no moduļa kopējā apjoma	3.1. Izpēte un analīze par tirgū pieejamie kiberdrošības risinājumiem: a) identitātes pārvaldībai, b) datu noplūdes prevencijai, c) priviliģeto lietotāju zuraudzībai; d) dinamiskai risku uzraudzībai.	Identificē un raksturo kiberdrošības risinājuma novērtēšanas kritērijus, nepieciešamāskiberdrošības pamatprasības	Sagatavo kiberdrošības risinājuma salīdzinošo rezultātu apkopojumu, prezentē rezultātu, mērījumus.	Interpretē un analizē kiberdrošības risinājuma salīdzinošos rezultātus, skaidro kritēriju nozīmi, pamato izvēlēta risinājuma priekšrocības.

Izprot: kiberdrošības parametru, mērījumus, veiktspējas rādījumu nozīmi konfigurācijas pārvaldībā, Gala ierīču (end-point) drošības līmeņa nozīmi kopējā drošības arhitektūrā, izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.					
4.Spēj:precīzi izpildīt testēšanas plānu,scenārijus, izmantojot atbilstošus rīkus un metodes sistēmu ievainojamību identificēšanai. **Zina: d**rošības testēšanas standartus un ietvarus; metodes un rīkus, kas atbalsta prasību apkopošanu un lēmumu pieņemšanas analīzi. Testēšanas ietekmi uz testējamajām IKT komponentēm, objektīva novērtējuma veikšanas paņēmienus, rīkus, matricas.	25% no moduļa kopējā apjoma	4.1.Testēšanas plāna un scenāriju izstrāde un izpilde.	Izpilda vienkāršu, sagatavotu drošības testēšanas plānu un scenārijus.	Izveido vienkāršu drošības testēšanas plānu un scenārijus konkrētam uzdevumam, koriģē esošu plānu atbilstoši riskiem.	Izveido un izpilda detalizētu drošības testēšanas plānu dažādām sistēmas komponentēm, prot veikt izmaiņas scenārijos, pielāgojot tos konstatētājiem riskiem.
		4.2.Testēšanas metožu un rīku pielietošana.	Izmanto automatizētu ievainojamību skenēšanas rīkus un interpretē to rezultātus. Izmanto vienkāršas tīkla skenēšanas metodes, lai noteiktu tīkla resursus.	Izmanto dažādus drošības testēšanas rīkus un kombinē to rezultātus, veic rezultātu analīzi un spēj tos interpretēt, identificē viltus pozitīvus rezultātus.	Manuāli pārbauda ievainojamības un veic testus, kas nav tikai automatizēti (piemēram, padziļināta Burp Suite analīze). Veic tīkla drošības testēšanu.

Izprot:dažādas drošības testēšanas metodikas (piem., OWASP). Dažādu IS ievainojamības (avotus, vektorus, tipoloģijas), dažādus drošības testēšanas rīkus un risinājumus.		4.3.Testēšanas rezultātu analīze un atskaišu sagatavošana.	Dokumentē testēšanas rezultātus, izmantojot iepriekš sagatavotu veidni. Raksturo un skaidro iegūtos rezultātus, pamato ievainojamību klasifikāciju.	Veido detalizētas atskaites, kurās apraksta atrastās ievainojamības, to ietekmi uz sistēmas darbību un piedāvā iespējamos risinājumus to novēršanā. Izmanto CVSS ievainojamību klasifikācijai.	Analizē un sasaista dažādas ievainojamības ar iespējamiem reālas dzīves uzbrukumiem. Demonstrē (*Proof of concept*) PoC un izskaidro ievainojamību cēloņus.

MODUĻA Kiberdrošības risinājumi (uzstādīšana, uzturēšana, novērtēšana) II APRAKSTS

Moduļa mērķis	Sniegt zināšanas un veicināt prasmes kiberdrošības risinājumos, to uzstādīšanā, uzturēšanā un novērtēšanā.
Moduļa uzdevumi	Attīstīt izglītojamo zināšanas un prasmes: 1. salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus (OT). 2. uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām.
Moduļa ieejas nosacījumi	Apgūts modulis "Kiberdrošības risinājumu uzstādīšana, uzturēšana, novērtēšana 1".
Moduļa apguves novērtēšana	Moduļa noslēgumā tiek kārtots noslēguma darbs - praktisks darbs, kurā balstoties uz situācijas aprakstu izglītojamais atlasa, salīdzina un piedāvā un ievieš konkrētu kiberdrošības risinājumu, kas būtu piemērots dotajai situācijai.
Moduļa nozīme un vieta kartē	Modulis "Kiberdrošības risinājumu uzstādīšana, uzturēšana, novērtēšana 2" ir "C" daļas modulis, kas paredzēts kā praktiskais mācību modulis pirmajai moduļa daļai.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Kiberdrošības risinājumi (uzstādīšana, uzturēšana, novērtēšana) II SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.Spēj: salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus (OT). **Zina:** Drošības sistēmu veidus, datu pārraides tīklu infrastruktūru un tās komponentes. **Izprot:** Izprot: izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.	50% no moduļa kopējā apjoma	1.1.Kiberdrošības risinājumu izvēle un ieviešana.	Izpēta informāciju un atlasa kiberdrošības risinājumu produktus un tiem atbilstošus analogus (tirgus analīze) t.sk. nestandarta, sarežģītām sistēmām, piemēram dalītās sistēmās, kiberfiziskās (angl. *Cyber-Physical*) sistēmās.	Apraksta kiberdrošības risinājumu īpašības un to analogus. Veic risinājumu salīdzināšanu t.sk. nestandarta, sarežģītām sistēmām, piemēram dalītās sistēmās, kiberfiziskās (angl. *Cyber-Physical*) sistēmās.	Izvērtē kiberdrošības risinājumu produktus un to analogus un izvēlas optimālāko risinājumu kā arī veic risinājuma uzstādīšanu t.sk. nestandarta, sarežģītām sistēmām, piemēram dalītās sistēmās, kiberfiziskās (angl. *Cyber-Physical*) sistēmās.
		1.2.Datu pārraides tīkli.	Pārzina datu pārraides tīkla infrastruktūru (topoloģijas, zonējumu) un tās komponentes (komutācijas, maršrutēšanas ierīces, serveri u.c.).	Veic datu pārraides tīklu infrastruktūru un to komponenšu drošu konfigurāciju.	Izvērtē datu pārraides tīklu infrastruktūras konfigurāciju un uzlabo tās drošību.
		1.3. Izmaiņu pārvaldība.	Izskaidro izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.	Izskaidro izmaiņu pārvaldības ietekmi darbības nepārtrauktības nodrošināšanā.	Izvēlas un pielieto situācijai piemērotākās izmaiņu ieviešanas metodes.
2.Spēj: uzturēt kiberdrošības risinājumus atbilstoši organizācijas drošības arhitektūras standartiem, drošības metrikām.	50% no moduļa kopējā apjoma	2.1. Kiberdrošības risinājumu uzturēšana.	Raksturo kiberdrošības risinājumus nestandarta, sarežģītām sistēmām, piemēram dalītās sistēmās, kiberfiziskās (angl. *Cyber-Physical*) sistēmās.	Izvērtē kiberdrošības risinājumus nestandarta, sarežģītām sistēmām, piemēram dalītās sistēmās, kiberfiziskās (angl. *Cyber-Physical*) sistēmās.	Ieviešun uztur kiberdrošības risinājumus nestandarta, sarežģītām sistēmām piemēram dalītās sistēmās, kiberfiziskās (angl.

Zina: drošības arhitektūras principus, to sastāvdaļas. **Izprot:** drošības metrikas un to nozīmi.					*Cyber-Physical*) sistēmās.
		2.2. Drošības arhitektūras standarti.	Izprot drošības arhitektūras standartus.	Izvērtē drošības arhitektūras standartus.	Pielieto drošības arhitektūras standartus.
		2.3. Drošības rādītāji.	Nosauc un apraksta drošības metrikas, mērījumus, rādītājus.	Izskaidro drošības metriku, mērījumu, rādītāju nozīmi.	Izvērtē drošības parametrus, metrikas usn to rādītājus.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA Kiberdrošības incidentu izmeklēšana II APRAKSTS

Moduļa mērķis	Nostiprināt un pilnveidot izglītojamo prasmes veikt kiberdrošības incidentu izmeklēšanu.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.apkopot nepieciešamo informāciju, kas saistīta ar iekšējās izmeklēšanas darbībām, piemērot atbilstošus incidentu izmeklēšanai nepieciešamos aizsardzības pasākumus. 2. sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta izmeklēšanā iesaistītajām pusēm, identificēt, apkopot un saglabāt digitālos pierādījumus, nodrošinot pierādījumu nemainīgumu (integritāti).
Moduļa ieejas nosacījumi	Apgūti visi A un B daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie prezentē divus dažādus izmeklēšanas procesa novērtējuma rezultātus.
Moduļa nozīme un vieta kartē	Modulis Kiberdrošības incidentu izmeklēšana II ir C daļas modulis, ko izglītojamie apgūst pēc B daļas moduļiem.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Kiberdrošības incidentu izmeklēšana II SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.**Spēj:**apkopot nepieciešamo informāciju, kas saistīta ar iekšējās izmeklēšanas darbībām, piemērot atbilstošus incidentu izmeklēšanai nepieciešamos aizsardzības pasākumus. **Zina:** izmeklēšanas darbību secību, pierādījumu apstrādes kārtību, digitālās izmeklēšanas metodes un rīkus, digitālo pierādījumu saglabāšanas principus, incidentu aptrādes dzīvesciklu, pierādījumu aptrādes dzīvesciklu. **Izprot:** dokumentācijas un būtisko atribūtu nozīmi incidentu izmeklēšanas un pierādījumu vākšanas procesā, digitālo pierādījumu apstrādes standartus, digitālo artefaktu apstrādes rīku darbības principus.	30% no moduļa kopējā apjoma	1.1. OSINT instrumenti, izmeklēšanas standarti, procedūras un sadarbība ar Valsts policiju	Raksturo digitālo pierādījumu veidus un juridiskos nosacījumus to ievākšanai.	Daļēji pielieto kriminālistikas metodoloģijas, saglabā pierādījumu ķēdi *(Chain of custody)* un ievēro juridiskās prasības.	Pilnībā pielieto kriminālistikas metodoloģijas, saglabā pierādījumu ķēdi un ievēro juridiskās prasības.
	30% no moduļa kopējā apjoma	1.2. Pierādījumu saglabāšana un uzticamības nodrošināšana	Saglabā digitālos pierādījumus pēc saviem ieskatiem, nenodrošinot datu ticamību, izmantojot dažus pierādījumu analīzes rīkus vadoties pēc instrukcijām.	Saglabā digitālos pierādījumus vadoties pēc parauga, nodrošinot datu ticamību, izmantojot vairākus pierādījumu analīzes rīkus vadoties pēc instrukcijām.	Saglabā digitālos pierādījumus saskaņā ar nozares standartiem, normatīviem aktiem, izmantojot vairākus pierādījumu analīzes rīkus, nodrošinot datu integritāti,
2.**Spēj:** sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar	40% no moduļa kopējā apjoma	2.1.Pretkriminalistikas metodes un manipulācijas ar pierādījumu	Atklāj dažas datu slēpšanas metodes (steganogrāfija, failu	Atklāj vairākas datu slēpšanas metodes (steganogrāfija, failu maskēšana, laika zīmju	Atklāj vairākas datu slēpšanas metodes (steganogrāfija, failu maskēšana, laika

incidenta izmeklēšanā iesaistītajām pusēm, identificēt, apkopot un saglabāt digitālos pierādījumus, nodrošinot pierādījumu nemainīgumu (integritāti). **Zina:** izmeklēšanas darbību secību, pierādījumu apstrādes kārtību, digitālās izmeklēšanas metodes un rīkus, digitālo pierādījumu saglabāšanas principus, incidentu aptrādes dzīvesciklu, pierādījumu aptrādes dzīvesciklu. **Izprot:** dokumentācijas un būtisko atribūtu nozīmi incidentu izmeklēšanas un pierādījumu vākšanas procesā, digitālo pierādījumu apstrādes standartus, digitālo artefaktu apstrādes rīku darbības principus.		integritāti (*Anti-Forensics & Evidence Tampering*)	maskēšana, laika zīmju manipulācija).	manipulācija); dokumentē kriminalistiskos atradumus.	zīmju manipulācija), nodrošinot datu integritāti, dokumentē kriminalistiskos atradumus, ievērojot juridiskās un ētiskās vadlīnijas.

Izmantotie avoti:

1. Cyber Security Body of Knowledge. (2021). *The Cyber Security Body of Knowledge (Version 1.1)*. University of Bristol. https://www.cybok.org/
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. https://www.cl.cam.ac.uk/~rja14/book.html
3. Valacich, J., Schneider, C., Hashim, M. (2023). Information Systems Today: Managing in the Digital World. 9th edition. Pearson Education Limited

MODUĻA Radio sakaru pamati APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo prasmes radiosakaru apgūšanai un izmantošanai dažādās situācijās, ievērojot drošība snoteikumus.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.veikt aprēķinus starp frekvenci un viļņa garumu. 2. atpazīt modulācijas veidu pēc spektra diagrammas. 3. definēt minimālās organizatoriskās prasības, lai varētu izveidot radiosakarus. 4. pārveidot vārdu uz/no fonētiskā alfabēta. 5. definēt kādā frekvenču joslā ir dotā frekvence vai kādas frekvences atbilst kurai frekvenču joslai. 6. izgatavot vienkāršu, harmonisku antenu dotā frekvencē. 7. sagatavoties eksāmenu radioamatiera apliecības saņemšanai. 8. identificēt elektrobīstamības un iekārtot radioamatiera staciju atbilstoši drošības noteikumiem.
Moduļa ieejas nosacījumi	Apgūti visi A un B daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie kārto kombinētu moduļa noslēguma darbu : teorētisko daļu un praktisko darbu – atbilstoši dažadu situāciju piedāvājiem.
Moduļa nozīme un vieta kartē	Modulis "Radio sakaru pamati" ir C daļas modulis.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Radio sakaru pamati SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis
1.**Spēj:** veikt aprēķinus starp frekvenci un viļņa garumu. **Zina:** radioviļņa definīciju un īpašības. **Izprot:** radioviļņa darbību.	1.Radioviļņu pamati. 12% no moduļa kopējā apjoma	1.1. Radioviļņa definīcija. 1.2 Jaudas aprēķini. 1.3 Radioviļņu spektrs. 1.4 Frekvenču joslas. 1.5 Radioviļņa garums.	Skaidro radioviļņu definīciju, to īpašības un darbību. Izskaidro aprēķinus starp frekvenci un viļņa garumu.	Apraksta un pamato radioviļņu definīciju, to īpašības un darbību. Aprēķina un analizē attiecības starp frekvenci un viļņa garumu.	Raksturo radioviļņu definīciju, to īpašības un darbību. Pielieto aprēķinus starp frekvenci un viļņa garumu. Izprot radioviļņu spectra diagrammu.
2.**Spēj:** atpazīt modulācijas veidu pēc spektra diagrammas. **Zina:** dažādu modulāciju plusus un mīnusus. **Izprot:** signāla apstrādes pamatprincipus.	2.Signālu modulācijas. 12% no moduļa kopējā apjoma	2.1 Amplitūdas modulācija. 2.2 Frekvences modulācija. 2.3 Vienas sānjoslas modulācija. 2.3 Fāzes modulācija. 2.4 Kvadratūras modulācija.	Nosauc signālu modulācijas veidus. Skaidro signāla apstrādes pamatprincipus. Atpazīst modulācijas veidu pēc spektra diagrammas.	Izskaidro signālu modulācijas veidus. Klasificē un raksturo signāla apstrādes pamatprincipu. Analizē un salīdzina modulācijas veidu pēc spektra diagrammas.	Ilustrē ar piemēriem signālu modulācijas veidus. Pamato signāla apstrādes pamatprincipus. Izvērtē modulācijas veidu pēc spektra diagrammas, raksturo to plusus un mīnusus.
3.**Spēj:** definēt minimālās organizatoriskās prasības, lai varētu izveidot radiosakarus. **Zina:** izmantotos terminus un to nozīmi, tipiskās kļūmes radiosakaru neesamības gadījumos. **Izprot:** veiksmīgu radiosakaru atkarību no apkārtējās vides faktoriem.	3.Radiosakaru organizācija. 12% no moduļa kopējā apjoma	3.1. Termini. 3.2 Kanālu veidi. 3.3 Radiodati. 3.4 Kļūmju noteikšana.	Izskaidro pielietojamos terminus, to nozīmi, biežākās problēmas radiosakaru neesamības gadījumos. Raksturo apkārtējās vides ietekmi uz radiosakariem.	Nosauc un raksturo pielietojamos terminus, to nozīmi, biežākās problēmas radiosakaru neesamības gadījumos. Izskaidro apkārtējās vides ietekmi uz radiosakariem. Atšķir un skaidro minimālās prasības, lai izveidotu radiosakarus	Pielieto un skaidro izmantojamos terminus, to nozīmi, biežākās problēmas radiosakaru neesamības gadījumos. Izvērtē apkārtējās vides ietekmi uz radiosakariem.

			Vispārīgi apraksta minimālās prasības, lai izveidotu radiosakarus.		Pamato ar piemēriem minimālās prasības, lai izveidotu radiosakarus.
4**.Spēj:** pārveidot vārdu uz/no fonētiskā alfabēta. **Zina:** NATO un latviešu fonētisko alfabētu. **Izprot:** fonētiskā alfabēta nozīmīgumu un pielietojumu.	4.Fonētiskais alfabēts. 5% no moduļa kopējā apjoma	4.1. NATO fonētiskais alfabēts. 4.2 Latviskais fonētiskais alfabēts. 4.3 Morzes kods.	Atpazīst NATO un latviešu fonētisko alfabētu. Skaidro fonētiskā alfabēta nozīmīgumu un pielietojumu. Apraksta vārdu pārveidošanas procesu uz/no fonētiskā alfabēta.	Atšķir un skaidro NATO un latviešu fonētisko alfabētu. Pamato fonētiskā alfabēta nozīmīgumu un pielietojumu. Izskaidro vārdu pārveidošanas procesu uz/no fonētiskā alfabēta.	Izvērtē atšķirības NATO un latviešu fonētiskajos alfabētos. Ilustrē ar piemēriem fonētiskā alfabēta nozīmīgumu un pielietojumu. Patstāvīgi pielieto vārdu pārveidošanas procesu uz/no fonētiskā alfabēta.
5**.Spēj:** definēt kādā frekvenču joslā ir dotā frekvence vai kādas frekvences atbilst kurai frekvenču joslai. **Zina:** radiofrekvenču joslas un tipiskās frekvenču īpašības katrā no joslām. **Izprot:** radioviļņu izplatīšanās veidus.	5.Radiofrekvenču īpašības. 12% no moduļa kopējā apjoma	5.1. Radiofrekvenču joslas. 5.2 Radiosakaru līdzekļu iedalījums. 5.3 Radioviļņu izplatības veidi 5.4 UĪV īpašības. 5.5 Radioviļņa apliekšanās. 5.6 Radio traucējumi.	Nosauc un apraksta radiofrekvenču joslas un to īpašības katrā no joslām. Raksturo radioviļņu izplatīšanās veidus. Raksturo frekvences atbilstību noteiktai frekvenču joslai.	Raksturo radiofrekvenču joslas un to īpašības katrā no joslām. Pamato radioviļņu izplatīšanās veidus. Raksturo un izskaidro frekvences atbilstību noteiktai frekvenču joslai.	Izvērtē radiofrekvenču joslas un to īpašības katrā no joslām. Salīdzina radioviļņu izplatīšanās veidus. Analizē frekvences atbilstību noteiktai frekvenču joslai.
6.Spēj: izgatavot vienkāršu, harmonisku antenu dotā frekvencē. **Zina:** populārāko antenu veidus un galvenos parametrus. **Izprot:** antenas būtiskumu veiksmīgu radiosakaru dibināšanā.	6.Antenas. 12% no moduļa kopējā apjoma	6.1. Antenas uzdevumi. 6.2 Antenu galvenie parametri. 6.3 Elektromagnētiskais lauks. 6.4 Antenu iedalījumi.	Atpazīst populārāko antenu veidus un to parametrus. Skaidro antenas nozīmi radiosakaru dibināšanā. Apraksta vienkāršu antenu izgatavošanas darbību secību dotā frekvencē.	Apraksts antenu veidus un to parametrus. Raksturo antenas nozīmi radiosakaru dibināšanā. Izskaidro darbību secību vienkāršu antenu izgatavošanā dotā frekvencē.	Atpazīst populārāko antenu veidus un to parametrus. Skaidro antenas nozīmi radiosakaru dibināšanā. Patstāvīgi izgatavo vienkāršu antenu dotā frekvencē.

		6.5 Antenu veidi un to īpašības. 6.6 Antenu efektivitātes uzlabošana. 6.7 Antenu izolatori.			
7**.Spēj:** sagatavoties eksāmenu radioamatiera apliecības saņemšanai. **Zina:** radioamatierisma pamatus, darbības kārtību un noteikumus. **Izprot**: tuvo un tālo radiosakaru būtiskumu krīzes situācijās.	7.Radioamatierisms. 25% no moduļa kopējā apjoma	7.1. Radioamatierisma definīcija. 7.2 Radioamatierisma vēsture. 7.3 Izsaukuma signāli. 7.4 Radioamatieru organizācijas. 7.5 Kā kļūt par radioamatieri. 7.6 QSL kartītes. 7.7 Radiosports. 7.8. Kolektīvās stacijas. 7.9 Radiosakaru prakse. 7.10 RST novērtējums. 7.11 Radiobākas. 7.12 Apaļais galds. 7.13 radioamatieru reģioni un zonas. 7.14 WW-lokators. 7.15 Azimutālā karte. 7.16 Radioamatiera "grāmatvedība" 7.17 Radioamatieru eksāmens.	Apraksta radioamatierisma pamatus, darbības kārtību un noteikumus. Skaidro tuvo un tālo radiosakaru būtiskumu krīzes situācijās. Vispārīgi apraksta radioamatiera eksāmena kārtošanas nosacījumus.	Izskaidro radioamatierisma pamatus, darbības kārtību un noteikumus. Orientējas tuvo un tālo radiosakaru būtiskumu krīzes situācijās. Izskaidro un pamato radioamatiera eksāmena kārtošanas nosacījumus.	Raksturo ar piemēriem radioamatierisma pamatus, darbības kārtību un noteikumus. Plāno un organizē tuvo un tālo radiosakarus krīzes situācijās. Uzskaita priekšrocības radioamatiera eksāmena kārtošanai.
8.Spēj: identificēt elektrobīstamības un iekārtot radioamatiera	8.Drošības nosacījumi strādājot ar radio.	8.1. Drošības tehnika.	Apraksta minimālās prasības izmantotajiem materiāliem	Nosauc un raksturo minimālās prasības izmantotajiem	Izvērtē minimālās prasības izmantotajiem

staciju atbilstoši drošības noteikumiem. **Zina:** minimālās prasības izmantotajiem materiāliem radioamatieru stacijas izbūvē. **Izprot:** elektrodrošības ievērošanas būtiskumu un nepieciešamību.	10% no moduļa kopējā apjoma	8.2. Vadu šķērsgriezumi un izolācijas. 8.3 Zemēšana. 8.4 Telpu dalījums pēc elektrobīstamības. 8.5 Instrumenti un aizsarglīdzekļi 8.6 Darbs augstumā. 8.7 Ugunsdrošības prasības. 8.8 Drošības prasības uzstādot mastu.	radioamatieru stacijas izbūvē. Izskaidro elektrodrošības ievērošanas nepieciešamību. Vispārīgi apraksta radioamatiera stacijas iekārtošanu atbilstoši drošības noteikumiem.	materiāliem radioamatieru stacijas izbūvē. Aprakta un pamato elektrodrošības ievērošanas nepieciešamību. Izskaidro radioamatiera stacijas iekārtošanu atbilstoši drošības noteikumiem.	materiāliem radioamatieru stacijas izbūvē. Izskaidro un pamato elektrodrošības ievērošanas nepieciešamību. Pamato ar piemēriem radioamatiera stacijas iekārtošanu atbilstoši drošības noteikumiem.

Izmantotie avoti:

1.MK noteikumi Nr.257 no 2023. gada 23.maija; Radioamatieru eksaminācijas apliecību un radioamatieru radiostacijas atļauju saņemšanas kārtība, kā arī radioamatieru radiostaciju lietošanas kārtība; https://likumi.lv/ta/id/342127-radioamatieru-eksaminacijas-apliecibu-un-radioamatieru-radiostacijas-atlauju-sanemsanas-kartiba-ka-ari-radioamatieru-radiostaciju-lietosanas-kartiba

2.Elektronisko sakaru likums; https://likumi.lv/ta/id/334345

3.Palīgmateriāls radioamatieriem drošības tehnikā; https://www.esakari.lv/lv/radioamatieru-eksamens4.Eiropas Pasta un telekomunikāciju konferences (CEPT) dokumenti:

CEPT rekomendācija T/R 61 – 01 CEPT radioamatieru atļauja

CEPT rekomendācija T/R 61 – 02 Saskaņotā radioamatieru pārbaudes apliecība

5.NATO fonētiskais alfabēts; https://www.nato.int/cps/nl/natohq/news_150391.htm

6.J.Baltins Radioamatierisms un amatieru sakaru prakse jautājumos un atbildēs; Valsts akciju sabiedrība "Elektroniskie sakari", 2019.gads,77.lpp.

MODUĻA Mākslīgā intelekta pamati APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas mākslīgā intelekta pielietošanā organizācijas kiberdrošības nodrošināšanā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. salīdzināt dažādus mākslīgā intelekta veidus un izskaidrot to pielietojumu. 2. Salīdzināt un izvērtēt dažādus MI algoritmus un to pielietojumu dažādās situācijās. 3. izvērtēt MI rīku efektivitāti uzbrukumu identificēšanā un pielietošanā kiberdrošības aizsardzības sistēmās. 4. analizēt drošības riskus MI sistēmās, izvērtējot Adversarial AI uzbrukumu metodes un sekas, argumentēti diskutēt par MI izmantošanas ētiskajiem un juridiskajiem aspektiem. 5. analizēt MI attīstības tendences kiberdošībā, izvērtējot jaunas darba iespējas, pielgojoties jaunajām prasībām MI inetgrācijai drošības procesu nodrošināšanā.
Moduļa ieejas nosacījumi	Apgūti A un B daļas moduļi.
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudījumu, kurā ir teorētisko zināšanu pārbaudes jautājumi un praktiskā darba daļa. Izglītojamie: 1. atbild uz testa jautājumiem. 2. veic scenārija analīzi, kurā ietverts viens būtisks drošības izaicinājums MI sistēmās, piedāvājot konkrētu risinājumu kiberdrošībā.
Moduļa nozīme un vieta kartē	Modulis " Mākslīgā intelekta pamati " ir C daļas modulis.
Satura īstenošanai izmantojamās mācību metodes	Darbs ar tekstu. Diskusija. Grupu darbs. Darbs ar informāciju. Projekta darbs. Aprēķinu veikšana. Situāciju analīze. Domu karte. Mācību ekskursija. Problēmu risināšana. Praktiskais darbs.

MODUĻA Mākslīgā intelekta pamati SATURS

Sasniedzamais mācīšanās rezultāts	Temats un sasniedzamā mācīšanās rezultāta īpatsvars %	Apakštemati	Mācību sasniegumu apguves līmeņu apraksti		
			Vidējs apguves līmenis	Optimāls apguves līmenis	Augsts apguves līmenis*
1.Spēj: salīdzināt dažādus mākslīgā intelekta veidus un izskaidrot to pielietojumu. **Zina:** mākslīgā intelekta vēsturisko attīstību un tā galvenos veidus. **Izprot:** Mākslīgā intelekta attīstību, un pielietojumu dažādās jomās.	1.1.Ievads mākslīgajā intelektā. 15% no moduļa kopējā apjoma	1.1.1.Mākslīgā intelekta (MI) definīcija un vēsture. 1.1.2.MI veidi	Apraksta MI un MI veidus. Raksturo MI vēsturiskos attīstības posmus. Uzskaita MI pielietojuma jomas.	Salīdzina MI veidus. Raksturo un pamato MI attīstības galvenos posmus. Raksturo MI pielietojumu dažādās jomās.	Salīdzina un izskaidro MI konceptus. Analizē MI veidus un tā pielietojumu dažādās jomās.
2.**Spēj:** izvērtēt dažādus MI algoritmus un to pielietojumu dotās situācijās. **Zina:** MI tehnoloģiju pamatprincipus, datu ieguves un apstrādes nozīmi un lomu MI darbībā. **Izprot:** Algoritmu ietekmi uz MI mācīšanos un lēmumu pieņemšanu.	2.1.MI tehnoloģijas un metodes 25% no moduļa kopējā apjoma	2.1.1.Datu ieguve un apstrāde MI sistēmās 2.1.2.Algoritmi un to loma mākslīgā intelekta darbībā	Apraksta pamata datu ieguves un apstrādes procesus. Atšķir dažādus MI algoritmus.	Raksturo datu ieguves un apstrādes nozīmi MI sistēmu darbībā. Raksturo dažādus MI algoritmus.	Pamato datu ieguves kvalitātes nozīmi un apstrādes ietekmi MI sistēmu darbībā. Piemēro MI algoritmus konkrētai, iepriekš dotai praktiskai situācijai.
3.Spēj: izskaidrot MI rīku efektivitāti uzbrukumu identificēšanā un pielietošanā kiberdrošības aizsardzības sistēmās. **Zina:** MI rīkus pielietojumu kiberdrošības uzbrukumu atklāšanā. **Izprot:** MI izmantošanu kiberdrošības uzbrukumu, tīkla drošības anomāliju, pikšķerēšanas uzbrukumu un	3.1.1MI pielietojums kiberdrošībā 25% no moduļa kopējā apjoma	3.1.1.MI pielietošana uzbrukumu atklāšanā 3.1.2.Tīkla drošības anomāliju noteikšana izmantojot MI rīkus. 3.1.3.Pikšķerēšanas uzbrukumu un ļaunprātīgu programmatūru	Apraksta MI darbību uzbrukumu atklāšanā. Apraksta MI rīkus tīkla drošības anomāliju noteikšanā. Atpazīst MI rīkus pikšķerēšanas un ļaunprātīgas programmatūras atpazīšanai.	Izskaidro MI palīdzību uzbrukumu atklāšanā. Izskaidro MI darbību tīkla datu analīzē. Salīdzina dažādas MI pieejas pikšķerēšanas un ļaunprātīgas programmatūras atpazīšanai.	Analizē MI risinājumu uzbrukumu atklāšanā stiprās un vājās puses. Raksturo MI darbību tīkla drošības analīzē un anomāliju noteikšanā. Pielieto MI rīkus pikšķerēšanas uzbrukumu un ļaunprātīgu

ļaunprātīgas programmatūras identificēšanā.		identificēšana, pielietojot MI rīkus.			programmatūru analīzē dotā scenārijā.
4.Spēj: analizēt drošības riskus MI sistēmās, izvērtējot Adversarial AI uzbrukumu metodes un sekas, argumentēti diskutēt par MI izmantošanas ētiskajiem un juridiskajiem aspektiem. **Zina:** galvenos drošības izaicinājumus un riskus MI sistēmās, ētiskos un juridiskos aspektus MI pielietošanai kiberdrošībā. **Izprot:** MI modeļu ļaunprātīgas manipulēšanas iespējas, datu aizsardzības ētiskos un juridiskos izaicinājumus.	4.1.Drošības izaicinājumi un riski MI sistēmās 25% no moduļa kopējā apjoma	4.1.1.Adversarial AI MI sistēmu maldināšana. 4.1.2.Datu privātums un drošība MI modeļos. 4.1.3.MI pielietošanas kiberdrošībā izaicinājumi. 4.1.4.Ētiskie un juridiskie aspekti MI izmantošanā.	Apraksta Adversarial AI ietekmi uz MI sistēmām. Atpazīst MI modeļu izraisītus datu privātuma apdraudējumus. Skaidro MI pielietošanas kiberdrošībā izaicinājumus. Skaidro ētiskos un juridiskos aspektus MI izmantošanā.	Izskaidro Adversarial AI uzbrukumus un to veidus. Izskaidro datu privātuma apdraudējumus MI modeļos. Salīdzina MI izaicinājumus kiberdrošībā. Apraksta dažādus ētiskos un juridiskos aspektus MI izmantošanā.	Analizē Adversarial AI uzbrukumu veidus un ietekmi. Pamato datu privātuma un drošības riskus MI modeļos. Izvērtē MI izmantošanas kiberdrošībā izaicinājumus. Argumentēti izskaidro ētiskā un juridiskā regulējuma nepieciešamību MI izmantošanā.
5.Spēj: analizēt MI attīstības tendences kiberdrošībā. **Zina:** MI attīstības tendences kiberdrošībā. **Izprot:** MI attīstības ietekmi kiberdrošības draudu atklāšanā un aizsardzības metožu izvēlē.	5.1.MI nākotne kiberdrošībā 10% no moduļa kopējā apjoma	5.1.1.MI attīstības tendences.	Apraksta MI attīstības tendences. Nosauc un apraksta MI rīku izmantošanu drošības nodrošināšanas automatizācijā.	Raksturo MI attīstības tendences. Salīdzina automatizācijas un MI lomu drošības procesu nodrošināšanā.	Analizē MI attīstības nākotnes tendences. Izvērtē un pamato MI automatizācijas plusus un mīnusus drošības procesu nodrošināšanā.

Izmantotie avoti:

1. M Šneps-Šneppe "Mākslīgais intelekts un kiberdraudi", izd. Jumava, 2024., 200.lpp
2. S.Russell, P.Norvig "Artifical Intelligence: A Modern Approach, Global Edition 4th edition, Pearson Education Limited, 2021, 1168 lpp.
3. T.Taulli "Artifical Intelligence Basics: A Non-Technical Introduction, Apress, 2019., 199.lpp.
4. M. Mitchell "Artifical Intelligence: A Guide for Thinking Humans", Farrar, Strauss and Giroux, 2019., 336.lpp
5. A.Chun-Chen Lui, O.Ming Kin Law, I.Law "Understanding Artifical Intelligence: Fundamentals and Applications", Wiley-IEEE Press, 2022., 224.lpp
6. I.Barkāne "Cilvēktiesību nozīme mākslīgā intelekta laikmet'\a: privātums, datu aizsardzība un regulējums masveida novērošanas novēršanai: monogrāfija.", Rīga, LU Akadēmiskais apgāds, 2023., 327.lpp
7. R.Kurzweil "The Singularity Is Nearer: Ehen We Merge with AI", Viking, 2024., 432.lpp

8. P.Olson “Supremacy: AI, ChatGPT, and the Race that Will Change the World”, St.Martin’s Press, 2024., 323.lpp
9. E.Mollick “Co-Intelligence: Living and Working with AI”, Portfolio, 2024., 253.lpp
10. M. Suleyman “The Coming Wave: Technology, Power and the Twenty-first Century’s Greatest Dilemma, Crown, 2023. 500.lpp.
11. N.Bostrom “Deep Utopia: Life and Meaning in a Solved World”, Indeapress Publishing, 2024., 538.lpp

MODUĻA Sabiedrības un cilvēka drošība (1.līmenis) APRAKSTS

Moduļa mērķis	Veicināt izglītojamo spējas un prasmes pieņemt fiziskajai, psihiskai un sociālajai drošībai un veselībai labvēlīgus lēmumus, preventīvi novērst nelaimes gadījumus sadzīvē un darbā, veidojot drošu un veselībai nekaitīgu apkārtējo vidi, lietot iegūtās zināšanas praksē.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Apzināties veselību kā kopveselumu un vērtību, saskatot personīgo un sabiedrības atbildību par katra cilvēka veselību. 2. Analizēt cilvēku rīcību, pieņemt atbildīgus lēmumus preventīvo pasākumu veikšanai drošas un veselībai nekaitīgas vides veidošanā un saglabāšanā. 3. Izvērtēt situāciju un sniegt pirmo palīdzību, nepieciešamības gadījumā izsaukt neatliekamo medicīnisko palīdzību un aprakstīt nelaimes gadījumu dispečeram. 4. Ievērot civilās aizsardzības rīcības plānus/instrukcijas, lai atbilstoši rīkotos dažādu katastrofu un apdraudējumu (t.sk. viltus ziņu) gadījumā, kā arī atskanot trauksmes sirēnai. 5. Atpazīt darba vides riskus un rīkoties atbilstoši darba aizsardzības prasībām. 6. Atpazīt ugunsnedrošas situācijas, preventīvi novērst ugunsgrēka izcelšanos, atbildīgi un droši rīkoties ugunsgrēka gadījumā, saskaņā ar ugunsdrošības noteikumiem un evakuācijas plānu. 7. Ievērot elektrodrošības noteikumus, lietojot elektroierīces un elektroiekārtas. 8. Analizēt pieejamo informāciju par vides kvalitāti Latvijā un pasaulē, rīkoties atbildīgi, saudzējot un racionāli izmantojot dabas resursus.
Moduļa ieejas nosacījumi	Apgūta pamatizglītība.
Moduļa apguves novērtēšana	Moduļa "Sabiedrības un cilvēka drošība (1. līmenis)" apguves noslēgumā izglītojamie kārto pārbaudījumu. Pārbaudījumā demonstrē visu modulī definēto sasniedzamo rezultātu apguvi. Pārbaudes darbā ietverta: 1) teorētisko zināšanu pārbaude (tests), iekļaujot jautājumus no visiem moduļa tematiem, 2) situāciju analīze (prezentācija) par iepriekš izvēlētu/izlozētu problēmjautājumu.
Moduļa nozīme un vieta kartē	Moduli "Sabiedrības un cilvēka drošība (1. līmenis)" īsteno kā mūžizglītības moduli profesionālās pamatizglītības, arodizglītības, profesionālās vidējās un profesionālās tālākizglītības programmās vai neformālās izglītības programmās. Modulis integrējams citos moduļos, ja tā saturs dublējas ar nozares profesionālās programmas moduļiem. Moduļa saturs, kas apgūstams obligātās veselības izglītības stundās, atbilstoši normatīvo aktu prasībām, netiek integrēts citos moduļos vai mācību priekšmetos. Pēc moduļa apguves var sekot moduļa "Sabiedrības un cilvēka drošība (2. līmenis)" apguve.

MODUĻA Sabiedrības un cilvēka drošība (1.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: izvērtēt informāciju par veselību ietekmējošiem faktoriem, apzināties personīgo un sabiedrības atbildību par katra cilvēka veselību. Zina: veselīga dzīvesveida paradumus un pasākumus, kas ietekmē personīgo un apkārtējo cilvēku veselību, kā arī riska faktorus un veicamos preventīvos pasākumus saslimšanas risku novēršanai vai mazināšanai. Izprot: veselību kā kopveselumu un vērtību, apzinās higiēnas būtību un nozīmi drošas un cilvēka veselībai nekaitīgas vides nodrošināšanā.	20% no moduļa kopēja apjoma	Nosauc riska faktorus, kas ietekmē veselību. Nosauc dzīves kvalitātes rādītājus. Uzskaita veselīgus paradumus. Nosauc būtiskākos veselības veicināšanas pasākumus. Nosauc riska faktorus, kuri ietekmē slimību rašanos un attīstību. Nosauc higiēnas pasākumus un darbības, lai slimības novērstu, apturētu to attīstību un mazinātu to radītās sekas. Vienkāršoti izskaidro vakcinācijas un kolektīvās imunitātes veidošanas nepieciešamību. Nosauc atkarību (t.sk. no vielām, procesiem un tehnoloģijām) veidus. Skaidro, kas ir atkarību profilakse. Uzskaita ar seksuālo un reproduktīvo veselību saistītās problēmas (t.sk. neplānota grūtniecība, seksuāli transmisīvās slimības), kā arī izsargāšanās metodes. Uzskaita nepieciešamās uzturvielas veselīgu ēšanas paradumu nodrošināšanā. Nosauc drošas un veselību veicinošas fiziskās aktivitātes. Nosauc ķermeņa masas indeksa aprēķināšanas formulu un skaidro veselīgas ķermeņa masas uzturēšanas nozīmi. Nosauc faktorus, kas ietekmē psihisko veselību. Nosauc, kur nepieciešamības gadījumā vērsties pēc palīdzības.	Izskaidro biežāko slimību riska faktorus (sirds un asinsvadu sistēmas slimību, elpceļu slimību, ļaundabīgo audzēju, spriedzes u.c. riska faktorus). Nosauc un raksturo dzīves kvalitātes rādītājus. Izskaidro nepieciešamību un savu atbildību īstenot veselīgu dzīvesveidu. Izskaidro veselības veicināšanas pasākumus (sabalansēts uzturs, optimāla fiziskā aktivitāte, psihiskā un reproduktīvā veselība, brīvība no atkarībām; atpūtas režīma ievērošana u.c.). Izskaidro riska faktorus, kuri ietekmē slimību rašanos un attīstību. Izskaidro nosacījumus un praktisko pasākumu kopumu, kas nepieciešams, lai samazinātu vai likvidētu vides faktoru (fizikālo, ķīmisko, bioloģisko) iespējami kaitīgo iedarbību. Pamato vakcinācijas nozīmi un kolektīvās imunitātes nozīmi. Klasificē atkarību veidus, raksturo to pazīmes un skaidro atkarību profilaksi. Skaidro ar seksuālo un reproduktīvo veselību saistītās problēmas un sekas, kā arī to profilaksi. Izskaidro nepieciešamo uzturvielu nozīmi veselības uzturēšanā. Pamato regulāru, sistemātisku un daudzveidīgu fizisko aktivitāšu nozīmi un ietekmi uz veselību, skaidro dopinga ietekmi uz organismu.

			Aprēķina savu ķermeņa masas indeksu un pamato veselīgas ķermeņa masas uzturēšanas nozīmi. Definē, kas ir psihiskā veselība, skaidro faktorus, kas to ietekmē. Pamatoti izklāsta viedokli par psihiskās veselības veicināšanas pasākumiem. Nosauc izplatītākos psihiskos traucējumus un skaidro, kur vērsties pēc palīdzības, ja ir raizes par savu un līdzcilvēku psihisko veselību.
2. Spēj: analizēt cilvēku rīcību, pieņemt atbildīgus lēmumus preventīvo pasākumu veikšanai drošas un veselībai nekaitīgas vides veidošanā un saglabāšanā. Zina: drošības un veselības riskus, nedrošu un bīstamu situāciju cēloņus, veicamos drošības pasākumus. Izprot: drošas uzvedības principu ievērošanas nozīmīgumu sadzīves un ārkārtas situācijās, kā arī savas personīgās rīcības nozīmi un atbildību nelaimes gadījumā.	10% no moduļa kopējā apjoma	Skaidro, kā pieņemtie lēmumi un rīcība ietekmē drošas un veselībai nekaitīgas vides veidošanu, prognozē lēmuma pieņemšanas un rīcības iespējamās sekas. Nosauc reāli notikušas sadzīves situācijas, kurās nācies pieņemt personīgu lēmumu riskēt vai izvēlēties drošību. Sniedz nedrošas rīcības piemērus dažādās dzīves situācijās, kuru rezultātā var ciest pats indivīds vai cits sabiedrības loceklis. Nosauc ikdienas iespējamās bīstamās situācijas, kuras var apdraudēt personīgo vai līdzcilvēku drošību, paskaidro iespējamos cēloņus un sekas. Nosauc izvēlētajā profesijā (nozarē) iespējamos drošības un veselības riskus, norāda dažus būtiskākos veicamos drošības pasākumus. Nosauc iespējamos riskus, dodoties uz ārzemēm. Skaidro apdrošināšanas nepieciešamību un min dažus	Analizē, kā pieņemtie lēmumi un rīcība ietekmē drošas un veselībai nekaitīgas vides veidošanu, minot piemērus, kā preventīvi novērst nedrošu un bīstamu situāciju rašanos un nelaimes gadījumus. Analizē reāli notikušas sadzīves situācijas, kurās nācies pieņemt personīgu lēmumu riskēt vai izvēlēties drošību. Prognozē iespējamās sekas, kas varēja rasties nepareizas izvēles gadījumā. Izskaidro cilvēku rīcību dažādās sadzīves un ārkārtas situācijās, prognozē iespējamās sekas, piedāvā risinājumus. Analizē ikdienas iespējamās bīstamās situācijas, kuras var apdraudēt personīgo vai līdzcilvēku drošību, skaidro cēloņus un sekas, piedāvā risinājumus drošības jautājumu uzlabošanai. Uzskaita un izskaidro izvēlētajā profesijā (nozarē) iespējamos drošības un veselības riskus norādot
3. Spēj: ievērot civilās aizsardzības rīcības plānus/ instrukcijas, lai atbilstoši rīkotos dažādu katastrofu un apdraudējumu (t.sk. viltus ziņu) gadījumā, kā arī atskanot trauksmes sirēnai.	15% no moduļa kopējā apjoma	Nosauc katastrofu veidus. Nosauc infekcijas slimību izplatīšanās riskus, t.sk. pārrobežu riskus, ietverot atbildību par savu un citu veselību. Nosauc epidēmiju un pandēmiju izplatības veidus un to pazīmes.	Raksturo katastrofu veidus, min piemērus Latvijā un pasaulē. Izskaidro nepieciešamo rīcību katastrofas gadījumā. Izskaidro infekcijas slimību izplatīšanās riskus, t.sk. pārrobežu riskus, ietverot atbildību par savu un citu veselību. Izskaidro epidēmiju un

Zina: dažādu ārkārtas un bīstamu situāciju pazīmes un atbilstošus civilās aizsardzības rīcības plānus/instrukcijas, kā arī paņēmienus viltus ziņu atpazīšanai un patiesas informācijas iegūšanai; individuālās aizsardzības līdzekļus un to lietošanu. Izprot: atbilstošas rīcības nozīmi ārkārtas situāciju, katastrofu gadījumā Latvijā un uzturoties ārpus tās.		Nosaka dabas katastrofu tuvošanos pēc pieejamās informācijas un rīkojas atbilstoši norādījumiem. Nosauc masu nekārtību un terorisma pazīmes. Nosauc pamatprincipus, kā jārīkojas ārkārtas situācijās. Nosauc vienu vai vairākas institūcijas, kur vērsties pēc palīdzības, ja ārkārtas situācijas laikā ir nodarīts kaitējums veselībai un drošībai. Atpazīst trauksmes sirēnu un vispārīgi apraksta, kā rīkoties un kur vērsties pēc palīdzības, tai atskanot. Nosauc paņēmienus, kā atpazīt viltus ziņas.	pandēmiju izplatības veidus, iespējamos cēloņus un sekas. Analizē pieejamo informāciju par dabas katastrofām, skaidro drošas rīcības soļus, izvērtē iespējamās sekas. Izskaidro, kāpēc rodas masu nekārtības, un argumentē, kāpēc tajās nevajag iesaistīties. Nosauc terorisma pazīmes un skaidro rīcību terorisma draudu gadījumā. Izskaidro būtiskākās atšķirības dažādās ārkārtas situācijās un skaidro rīcību katrā konkrētajā gadījumā. Nosauc vairākas institūcijas, kur vērsties pēc palīdzības, ja ārkārtas situācijas laikā ir nodarīts kaitējums veselībai un drošībai vai radīti būtiski materiālie zaudējumi. Pamato savu viedokli. Skaidro, kur atrodas skolai un dzīvesvietai tuvākā trauksmes sirēna un droša pulcēšanās vieta. Pamatoti izklāsta savu viedokli, kā pareizi rīkoties, atskanot trauksmes sirēnai, kur un pie kā vērsties pēc palīdzības. Atpazīst viltus ziņas un izskaidro to radītās sekas.
[1]4. Spēj: atpazīt darba vides riskus un rīkoties atbilstoši darba aizsardzības prasībām. Zina: darba vides riska faktorus, iespējamos kaitējumus, risku faktoru novēršanas preventīvos pasākumus (t.sk. obligātās veselības pārbaudes, vakcinācija u.c.), darba devēja un nodarbināto pienākumus (t.sk. veselības un dzīvības saglabāšanā), tiesības un atbildību darba aizsardzības jomā.	20% no moduļa kopējā apjoma	Nosauc darba aizsardzības mērķi un pasākumus tā sasniegšanai. Nosauc darba devēja un darbinieka galvenos pienākumus un tiesības darba aizsardzības jomā. Skaidro darba aizsardzības speciālista lomu uzņēmumā. Nosauc būtiskākās darba aizsardzības prasības un darba devēja veicamos pasākumus. Nosauc darba vides riskus un to konstatēšanas metodes. Nosauc fizikālo darba vides riska faktoru novēršanas principus. Nosauc fizisko darba vides riska faktoru novēršanas principus un min	Skaidro darba aizsardzības mērķi un nosauc darba aizsardzības likumā minētos pasākumus mērķa sasniegšanai. Izskaidro darba devēja pienākumus un tiesības darba aizsardzības jomā. Saista valsts un uzņēmuma ekonomisko stāvokli ar darba aizsardzības pasākumu īstenošanu. Nosauc un izskaidro darba aizsardzības speciālista pienākumus. Analizē darba aizsardzības prasības un skaidro veicamos darba aizsardzības pasākumus. Lieto konkrētu metodi darba vides risku novērtēšanā.

Izprot: darba aizsardzības būtību un tās nozīmi, darba vides risku faktoru mazināšanas vai novēršanas pasākumu nepieciešamību.			
5. Spēj: atpazīt ugunsnedrošas situācijas, preventīvi novērst ugunsgrēka izcelšanos, atbildīgi un droši rīkoties ugunsgrēka gadījumā, saskaņā ar ugunsdrošības noteikumiem un evakuācijas plānu. Zina: ugunsgrēka izcelšanās iemeslus, degšanas veidus, ugunsgrēka novēršanas iespējas, preventīvi veicamos pasākumus. Izprot: ugunsgrēka bīstamību un preventīvi veicamo pasākumu nozīmi.	10% no moduļa kopējā apjoma	Sniedz piemērus, kāpēc izceļas ugunsgrēks. Nosauc ugunsgrēku klases. Nosauc degšanas veidus. Nosauc svarīgākos preventīvos pasākumus, lai novērstu ugunsgrēka izcelšanos. Nosauc ugunsdzēsības aparātu iedalījumu. Nosauc Valsts ugunsdzēsības un glābšanas dienesta tālruņa numuru un saviem vārdiem apraksta situāciju dispečeram. Nosauc konkrētus rīcības soļus, atskanot trauksmes signālam. Orientējas evakuācijas plānā, pareizi norāda evakuācijas virzienus un ceļus.	Izskaidro cilvēku rīcības ietekmi uz ugunsgrēka izcelšanos. Nosauc un izskaidro ugunsgrēku klases. Nosauc un izskaidro degšanas veidus. Izskaidro svarīgākos preventīvos pasākumus, lai novērstu ugunsgrēka izcelšanos un tālāku izplatību. Izskaidro, kādā gadījumā lieto attiecīgos ugunsdzēsības aparātus, izvēlas piemērotus ugunsdzēsības līdzekļus. Izskaidro, kā izsaukt Valsts ugunsdzēsības un glābšanas dienestu un kādā secībā jāsniedz informācija dispečeram. Detalizēti izskaidro, kā jārīkojas, atskanot trauksmes signālam, pamato savu viedokli. Identificē nepilnības evakuācijas plānos, veic labojumus tā, lai atbilstoši norādēm būtu iespējams droši izkļūt no telpām.
6. Spēj: ievērot elektrodrošības noteikumus, lietojot elektroierīces un elektroiekārtas. Zina: būtiskākos darba drošības noteikumus darbā ar elektroierīcēm un elektroiekārtām, elektriskās strāvas iedarbību uz cilvēka organismu, veicamos pasākumus elektrotraumu nepieļaušanai vai mazināšanai; palīdzības	10% no moduļa kopējā apjoma	Nosauc elektrisko strāvu raksturojošos lielumus (spriegums, strāvas stiprums, pretestība, jauda) un to mērvienības. Nosauc strāvas iedarbības uz cilvēka organismu noteicošos faktorus. Skaidro jēdzienu "soļa spriegums" un raksturo, kā rīkoties soļa sprieguma gadījumā. Nosauc elektrotraumu mazināšanas pasākumus. Nosauc rīcības secību cietušā atbrīvošanai no elektriskās strāvas iedarbības. Nosauc būtiskākos darba drošības noteikumus darbā ar elektroierīcēm un elektroiekārtām.	Nosauc elektrisko strāvu raksturojošos lielumus (spriegums, strāvas stiprums, pretestība, jauda) un to mērvienības. Veic vienkāršus aprēķinus. Skaidro, kas ir pazeminātie spriegumi, aizsargzemējums, drošinātāji, strāvas automāti Raksturo strāvas iedarbības uz cilvēka organismu noteicošos faktorus. Izskaidro, kā faktoru izmaiņas ietekmē iedarbību uz organismu. Pamato "soļa sprieguma" rašanos un savu rīcību soļa sprieguma gadījumā. Izskaidro nepareizas rīcības sekas. Izskaidro elektrotraumu mazināšanas pasākumus, pamato to nepieciešamību.

sniegšanu elektrotraumu gadījumā. Izprot: elektroierīču un elektroiekārtu drošas lietošanas nozīmi veselības saglabāšanā.			Izskaidro rīcības secību cietušā atbrīvošanai no strāvas iedarbības, paskaidro iespējamās sekas. Izskaidro darba drošības noteikumus darbā ar elektroierīcēm un elektroiekārtām.
[2]7. Spēj: analizēt pieejamo informāciju par vides kvalitāti Latvijā un pasaulē, rīkoties atbildīgi, saudzējot un racionāli izmantojot dabas resursus. Zina: vides aizsardzības pamatprincipus, iespējamos kaitējuma draudus videi un veicamos preventīvos pasākumus. Izprot: situāciju vides aizsardzībā Latvijā un pasaulē, dabas resursu saudzīgas izmantošanas būtību un ilgtspējīgas saimniekošanas nozīmi apgūstamajā tautsaimniecības nozarē.	15% no moduļa kopējā apjoma	Nosauc vides aizsardzības pamatprincipus Latvijā. Nosauc dabas resursus. Izskaidro dabas resursu saudzīgas izmantošanas veidus. Nosauc atkritumu saimniecības pamatprincipus. Izskaidro atkritumu savākšanas un utilizēšanas procesa nepieciešamību apgūstamajā tautsaimniecības nozarē. Sniedz piemērus par saudzīgu attieksmi pret dabu. Nosauc ekoloģiskos izstrādājumus un materiālus, nosauc ekoinovācijas pasaulē un Latvijā. Skaidro jēdzienus "atjaunojamā enerģija", "alternatīvā enerģija".	Izskaidro vides aizsardzības pamatprincipus un vispārējos Latvijas vides ilgtspējīgas attīstības pasākumus. Klasificē dabas resursus pēc to daudzuma, pieejamības. Izvērtē to racionālu izmantošanu, neapdraudot nākamo paaudžu vajadzības. Izskaidro katra dabas resursa būtību, ieguves iespējas un saudzīgas izmantošanas veidus. Izskaidro atkritumu saimniecības pamatprincipu būtību, šķirošanas procesa nepieciešamību, otrreizējo izejvielu pārstrādes nepieciešamību un inovācijas atkritumu pārstrādē apgūstamajā tautsaimniecības nozarē.

Izmantojamie avoti:

1. Aizsargjoslu likums [skatīts 2020. gada 10.martā]. Pieejams: *http://likumi.lv/doc.php?id=42348*
2. Animācijas filmas par darba vides jautājumiem [skatīts 2020. gada 10.martā]. Pieejams: *https://www.napofilm.net/lv/napos-films/films*
3. Atgādne nodarbinātajiem par elektromagnētisko lauku [skatīts 2020. gada 10.martā]. Pieejams: *http://www.vdi.gov.lv/files/atgadne_elektromagnetiskais_lauks_final(1).pdf*
4. Atgādne nodarbinātajiem par vibrāciju [skatīts 2020. gada 10.martā]. Pieejams: *http://petijumi.mk.gov.lv/sites/default/files/file/atgadne_Vibracija.pdf*
5. Atgādne nodarbinātajiem, kas pakļauti bioloģiskajiem riskiem [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/atgadne-biologiskie-riski.pdf*
6. Bambergs K. Ģeoloģija un hidroģeoloģija. Rīga: Zvaigzne, 1993.

7. Biotopu rokasgrāmata. Rīga: Preses nams, 2000.
8. Civilā aizsardzība. Minimālās prasības civilās aizsardzības kursa saturam vispārējā un profesionālajā izglītībā. Prezentācija [skatīts 2020. gada 10.martā]. Pieejams: *https://visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/civila_aizsardziba.pdf*
9. Civilās aizsardzības un katastrofas pārvaldīšanas likums [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/282333-civilas-aizsardzibas-un-katastrofas-parvaldisanas-likums*
10. Clapham W. B., JR. Natural ecosystems. New York: Macmillan Publishing Co., Inc.,1993.
11. Darba aizsardzības apmācību metodes. – Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Darba_aizsardzibas_apmacibas_metodes.pdf*
12. Darba aizsardzības likums [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=26020*
13. Darba devēja rokasgrāmata. – Rīga: Latvijas Darba devēju konfederācija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://www.lm.gov.lv/upload/darba_devejiem/darb_dev_rok.pdf*
14. Darba drošība. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Darba_drosiba.pdf*
15. Darba higiēna. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Darba_higiena.pdf*
16. Dokumentālā filma "Dabas stihijas" 1. epizode [skatīts 2020. gada 10.martā]. Pieejams: *www.youtube.com/watch?v=X4hbDsdNg5k*
17. Drošības prasības, veicot darbus elektroietaisēs [skatīts 2020. gada 10.martā]. Pieejams: *http://www.vdi.lv/admin/files/info%20materiaali/1.1.pdf*
18. Ergonomika darbā. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Ergonomika.pdf*
19. Gavrilova G. Jūraszāles. Latvijas daba. Rīga: Latvijas enciklopēdija, 1995.
20. Grīnberga M., Rīdūze L., Veģere I. Cilvēks vidē. Rīga: Zvaigzne, 2004.
21. Hakanson L., Physical geography of the Baltic. The Baltic Sea Environment: 1. Uppsala University, Uppsala, Sweden, 1993.
22. Ministru kabineta 2017. gada 5. decembra noteikumi Nr. 716 "Minimālās prasības obligātā civilās aizsardzības kursa saturam un nodarbināto civilās aizsardzības apmācības saturam" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/295896-minimalas-prasibas-obligata-civilas-aizsardzibas-kursa-saturam-un-nodarbinato-civilas-aizsardzibas-apmacibas-saturam-*
23. Ministru kabineta 2016. gada 19. aprīļa noteikumi Nr. 238 "Ugunsdrošības noteikumi" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/281646-ugunsdrosibas- noteikumi*
24. Ministru kabineta 2010. gada 10. augusta noteikumi Nr. 749 "Apmācības kārtība darba aizsardzības jautājumos" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=214922*
25. Ministru kabineta 2008. gada 25. marta noteikumi Nr. 195 "Mašīnu drošības noteikumi" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=173016*
26. Ministru kabineta 2009. gada 10. marta noteikumi Nr. 219 "Kārtība, kādā veicama obligātā veselības pārbaude" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=189070*
27. Ministru kabineta 2007. gada 2. oktobra noteikumi Nr. 660 "Darba vides iekšējās uzraudzības veikšanas kārtība" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=164271*
28. Ministru kabineta 2007. gada 28. augusta noteikumi Nr. 568 "Kārtība, kādā noformējams administratīvā pārkāpuma protokols-paziņojums par mehānisko transportlīdzekļu pārvietošanās noteikumu pārkāpšanu ārpus autoceļiem Baltijas jūras un Rīgas jūras līča piekrastes krasta kāpu

aizsargjoslā, pludmalē vai īpaši aizsargājamā dabas teritorijā" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/163021-kartiba-kada-noformejams-administrativa-parkapuma-protokols-pazinojums-par-mehanisko-transportlidzeklu-parvietosanas*
29. Ministru kabineta 2002. gada 9. decembra noteikumi Nr. 526 "Darba aizsardzības prasības, lietojot darba aprīkojumu un strādājot augstumā" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=69282&version_date=02.06.2007&from=off*
30. Ministru kabineta 2002. gada 17. septembra noteikumi Nr. 427 "Uzticības personu ievēlēšanas un darbības kārtība" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=66827*
31. Ministru kabineta 2002. gada 3. septembra noteikumi Nr. 400 "Darba aizsardzības prasības drošības zīmju lietošanā" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=66071*
32. Ministru kabineta 2002. gada 20. augusta noteikumi Nr. 372 "Darba aizsardzības prasības, lietojot individuālos aizsardzības līdzekļus" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=65619*
33. NAPO filmas [skatīts 2020. gada 10.martā]. Pieejams: *https://www.napofilm.net/lv/napos-films/films?page=1&view_mode=page_grid*
34. Ogļhidrāti uzturā. [skatīts 2020. gada 10.martā]. Pieejams:http://www.vm.gov.lv/lv/tava_veseliba/veseligs_uzturs/oglhidrati/
35. Olbaltumvielas uzturā. [skatīts 2020. gada 10.martā]. Pieejams: http://www.vm.gov.lv/lv/tava_veseliba/veseligs_uzturs/olbaltumvielas/
36. Pastors A. Baltijas jūras piekraste un Rīgas jūras līcis. Latvijas ģeogrāfija. Rīga: Zinātne, 1997.
37. Plakāts mīts "Darba aizsardzība ir tikai darba devēja uzdevums" [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/darba-aizsardziba-ir-lieki-izdevumi.pdf*
38. Plakāts mīts "Darba aizsardzība ir tikai lieki izdevumi" [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/darba-aizsardziba-ir-lieki-izdevumi.pdf*
39. Plakāts "Nepaej garām – ziņo par riskiem darba vietā!" [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/11/15_2010_Plakats_A2_Zino_par_riskiem_final.pdf*
40. Psihosociālā darba vide. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/psihosocialadarbavide.pdf*
41. Skolas vecuma bērnu un pusaudžu veselība [skatīts 2020. gada 10.martā]. Pieejams: *https://spkc.gov.lv/upload/Petijumi%20un%20zinojumi/Sabiedribas%20veselibas%20petijumi/skolas_vecuma_bernu_un_pusaudzu_veseliba_svs_4merka_izvertejums_2008.pdf*
42. Slimību profilakses un kontroles centra tīmekļa vietne. Informatīvi materiāli. [skatīts 2020. gada 10.martā]. Pieejams: https://spkc.gov.lv/lv/informativi-izdevumi
43. Slimību profilakses un kontroles centra sagatavotās izglītojošās filmas [skatīts 2020. gada 10.martā]. Pieejams: *https://www.spkc.gov.lv/lv/informativi-izdevumi/izglitojosas-filmas*
44. Stola I., Siliņš M. Veselības mācība vidusskolai. Rīga: RaKa, 2005.
45. Sugu un biotopu aizsardzības likums [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=3941*
46. Ministru kabineta 2002. gada 9. decembra noteikumi Nr. 526 "Darba aizsardzības prasības, lietojot darba aprīkojumu un strādājot augstumā" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=69282&version_date=02.06.2007&from=off*

MODUĻA Sabiedrības un cilvēka drošība (2. līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas un prasmes pieņemt fiziskajai, psihiskai un sociālajai drošībai un veselībai labvēlīgus lēmumus, preventīvi novērst nelaimes gadījumus sadzīvē un darbā, veidojot drošu un veselībai nekaitīgu apkārtējo vidi, lietot iegūtās zināšanas praksē.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Izvēlēties valsts vai pašvaldības institūcijas, kurās vērsties pēc palīdzības sabiedrības drošības jomā, sameklēt atbildīgās institūcijas/personas kontaktinformāciju un sazināties ar to. 2. Raksturot drošu un veselībai nekaitīgu darba vidi, analizēt nelaimes gadījumu darbā un arodslimību rašanās iemeslus. 3. Pieņemt savai un līdzcilvēku fiziskajai un garīgajai veselībai labvēlīgus lēmumus, īstenot tos. 4. Novērtēt situāciju vides aizsardzības jomā, lai ievērotu un popularizētu zaļās domāšanas principus.
Moduļa ieejas nosacījumi	Apgūta moduļa "Sabiedrības un cilvēka drošība (1. līmenis)" programma.
Moduļa apguves novērtēšana	Moduļa "Sabiedrības un cilvēka drošība (2.līmenis)" apguves noslēgumā izglītojamie kārto pārbaudījumu. Pārbaudījumā demonstrē visu modulī definēto sasniedzamo rezultātu apguvi. Pārbaudījumā tiek iekļauti: 1) teorētisko zināšanu pārbaude (tests), ietverot jautājumus par visiem moduļa tematiem, 2) pētnieciskais darbs par kādu modulī apskatītu tematu/problēmu.
Moduļa nozīme un vieta kartē	Moduli „Sabiedrības un cilvēka drošība (2. līmeni)" īsteno kā mūžizglītības moduli profesionālās vidējās un profesionālās tālākizglītības programmās. Moduļa saturs, kas apgūstams obligātās veselības izglītības stundās, atbilstoši normatīvo aktu prasībām, netiek integrēts citos moduļos vai mācību priekšmetos.

MODUĻA Sabiedrības un cilvēka drošība (2. līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: izvēlēties valsts vai pašvaldību institūcijas, kurās vērsties pēc palīdzības sabiedrības drošības jomā, sameklēt atbildīgās institūcijas/ personas kontaktinformāciju un sazināties ar to. Zina: valsts un pašvaldību institūciju darbības virzienus un galvenās funkcijas sabiedrības drošības jautājumu risināšanā. Izprot: valsts un pašvaldību institūciju lomu sabiedrības drošības jautājumu risināšanā.	10% no moduļa kopējā apjoma	Nosauc valsts un pašvaldību institūcijas, kas veic uzraudzību sabiedrības drošības jomā.	Identificē valsts un pašvaldību institūcijas, kas veic uzraudzību sabiedrības drošības jomā, izskaidro to darbības virzienus, minot piemērus.
		Nosauc Valsts ugunsdzēsības un glābšanas dienesta darbības pamatvirzienus un galvenās funkcijas.	Raksturo ar piemēriem Valsts ugunsdzēsības un glābšanas dienesta darbības virzienus, galvenās funkcijas un tiesības.
		Nosauc Valsts policijas un pašvaldības policijas darbības pamatvirzienus un galvenās funkcijas.	Izskaidro ar piemēriem Valsts policijas un pašvaldības policijas darbības virzienus, galvenās funkcijas un tiesības.
		Nosauc Neatliekamās medicīniskās palīdzības dienesta darbības pamatvirzienus un galvenās funkcijas. Apraksta situācijas, kurās nepieciešams vērsties pie ģimenes ārsta, paskaidro kā sazināties ar viņu un/vai pierakstīties vizītei.	Raksturo ar piemēriem Neatliekamās medicīniskās palīdzības dienesta darbības virzienus un galvenās funkcijas. Ar piemēriem skaidro situācijas, kurās jāvēršas pie ģimenes ārsta, nosauc veidus kā sazināties ar viņu un/vai pierakstīties vizītei, paskaidro ģimenes ārsta lomu saslimšanu diagnostikā un ārstēšanā.
		Nosauc Zemessardzes darbības pamatvirzienus un galvenās funkcijas.	Raksturo ar piemēriem Zemessardzes darbības virzienus un galvenās funkcijas.
2. Spēj: veidot drošu un veselībai nekaitīgu darba vidi, analizēt nelaimes gadījumu darbā un arodslimību rašanās iemeslus. Zina: darba aizsardzības organizēšanas un uzraudzīšanas pamatprincipus, nozarei specifiskos darba vides	50% no moduļa kopējā apjoma	Nosauc darba aizsardzības sistēmas uzraudzības posmus, veicamās darbības un galvenos darba aizsardzību reglamentējošos dokumentus.	Izskaidro katrā darba aizsardzības sistēmas uzraudzības posmā veicamās darbības un analizē normatīvajos dokumentos atrodamo informāciju.
		Nosauc nozarei specifiskos iespējamos darba vides riskus, to ietekmi uz veselību un saistību ar obligātajām veselības pārbaudēm. Vispārīgi apraksta konkrētu situāciju darba vides risku noteikšanai un novēršanai. Raksturo darba aizsardzības līdzekļu lietošanas nepieciešamību darbinieku veselības saglabāšanai.	Nosauc un skaidro nozarei specifiskos iespējamos darba vides riskus, to ietekmi uz veselību un saistību ar obligātajām veselības pārbaudēm. Analizē konkrētu situāciju darba vides risku noteikšanai un novēršanai. Raksturo darba aizsardzības līdzekļu lietošanas nepieciešamību darbinieka veselības saglabāšanai.

riskus, to novēršanas vai samazināšanas pasākumus. Izprot: darba aizsardzības sistēmas būtību.		Nosauc darba aizsardzības prasību neievērošanas sekas (nozarei specifiskos nelaimes gadījumus darbā, arodslimības).	Izskaidro nelaimes gadījumu un arodslimību rašanās cēloņus.
3. Spēj: pieņemt savai un līdzcilvēku fiziskajai un psihiskajai veselībai labvēlīgus lēmumus, īstenot tos. Zina: veselīga dzīvesveida principus, iespējamos riska faktorus (t.sk. pašvērtējums, sociālā vide, izdegšanas sindroms), psihosomatiskos traucējumus, to cēloņus, izpausmes un profilakses pasākumus, zina, kur vērsties pēc palīdzības. Izprot: veselīga dzīvesveida principus (t.sk. fiziskās un psihiskās veselības savstarpējo vienotību) un profilakses pasākumu nozīmīgumu.	20% no moduļa kopējā apjoma	Nosauc savas rīcības piemērus, kas var ietekmēt personīgo vai citu cilvēku veselību. Izstāsta, kur un pēc kādas palīdzības vērsties. Izskaidro, kas ir savai un līdzcilvēku veselībai labvēlīgs lēmums.	Minot konkrētus piemērus, izskaidro saikni starp rīcību un tās radītajām sekām - slimību attīstību. Skaidro veselībai labvēlīgu lēmumu pieņemšanas un to īstenošanas nozīmību.
		Nosauc sociālos riska faktorus, kas spēj ietekmēt fizisko un psihisko veselību.	Nosauc un izskaidro sociālos riska faktorus, kas spēj ietekmēt fizisko un psihisko veselību. Analizē situāciju cēloņus un sekas.
		Nosauc piemērus, kā pašvērtējums ietekmē veselību veicinošu dzīvesveidu.	Nosauc piemērus un izskaidro, kā pašvērtējums ietekmē veselību veicinošu dzīvesveidu.
		[1]Skaidro, kas ir veselīgs dzīvesveids (t.sk. fiziskās un psihiskās veselības savstarpējo ietekmi). Nosauc psihosomatiskos traucējumus un to cēloņus.	[1] Pamato veselīga dzīvesveida (t.sk. fiziskās un psihiskās veselības) nozīmīgumu. Raksturo ar piemēriem psihiskās veselības ietekmējošos faktorus (piem., bioloģiskie faktori, ārējie faktori, pieredze). Izskaidro, kas ir psihosomatiskās slimības un kāda ir to profilakse.
		[1]Nosauc izdegšanas sindroma un garīgās pārslodzes izpausmes.	[1] Izskaidro izdegšanas sindroma un garīgās pārslodzes cēloņus, izpausmes un profilaksi.
		Nosauc jautājumus, kas jāuzdod ārstam vai farmaceitam par medikamentu drošu lietošanu. Skaidro, kas ir medikamentu (t.sk. pretsāpju zāļu, antibiotiku) atbildīga lietošana, ko nozīmē rezistences veidošanās.	Nosauc jautājumus, kas jāuzdod ārstam vai farmaceitam par medikamentu drošu lietošanu, un pamato savu jautājumu izvēli. Skaidro medikamentu (t.sk. pretsāpju zāļu, antibiotiku) atbildīgas lietošanas nozīmi un rezistences veidošanos.
[2]4. Spēj: novērtēt situāciju vides aizsardzības jomā, lai ievērotu un popularizētu zaļās domāšanas principus. Zina: tautsaimniecības nozaru vides kvalitātes pamatprasības, kaitējuma	20% no moduļa kopējā apjoma	Nosauc vides aizsardzības problēmas pasaulē, ES un Latvijā.	Raksturo svarīgākās vides aizsardzības deklarācijas, konvencijas un direktīvas.
		Nosauc tautsaimniecības nozares, kurās ir jāveic vides aizsardzības pasākumi, akcentējot vides aizsardzības pasākumus apgūstamajā (profesijā) nozarē.	Raksturo tās tautsaimniecības nozares, kurām ir jāpievērš lielāka uzmanība vides uzraudzībā. Izskaidro vides aizsardzības pasākumu nepieciešamību apgūstamajā (profesijā) nozarē.

draudus videi un veicamos preventīvos pasākumus. Izprot: vides aizsardzības problemātiku pasaulē un Latvijā, svarīgāko vides aizsardzības deklarāciju, konvenciju un direktīvu nozīmi vides ilgtspējīgas attīstības veidošanā.			
[3]5. Spēj: atbildīgi pieņemt lēmumus par darba tiesisko attiecību uzsākšanu, darba uzdevumu veikšanu un darba tiesisko attiecību izbeigšanu. Zina: darba tiesību pamatjautājumus. Izprot: darba tiesisko attiecību normatīvā regulējuma nozīmīgumu.		Formulē darba tiesību regulējuma pamatus, darbinieka tiesības un pienākumus, darba devēja tiesības un pienākumus. Apraksta kolektīvo darba tiesību būtību, to nozīmi; darbinieka un darba devēja attiecību regulējumu.	Skaidro darba tiesību regulējumu, darba līguma būtību un nozīmi. Skaidro kolektīvo darba tiesību būtību un nozīmi; izstrādā priekšlikumus darbinieka un darba devēja attiecību regulējumam

Izmantojamie avoti:

1. Aizsargjoslu likums [skatīts 2020. gada 10.martā]. Pieejams: *http://likumi.lv/doc.php?id=42348*
2. Animācijas filmas par darba vides jautājumiem [skatīts 2020. gada 10.martā]. Pieejams: *https://www.napofilm.net/lv/napos-films/films*
3. Atgādne nodarbinātajiem par elektromagnētisko lauku [skatīts 2020. gada 10.martā]. Pieejams: *http://www.vdi.gov.lv/files/atgadne_elektromagnetiskais_lauks_final(1).pdf*
4. Atgādne nodarbinātajiem par vibrāciju [skatīts 2020. gada 10.martā]. Pieejams: *http://petijumi.mk.gov.lv/sites/default/files/file/atgadne_Vibracija.pdf*
5. Atgādne nodarbinātajiem, kas pakļauti bioloģiskajiem riskiem [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/atgadne-biologiskie-riski.pdf*
6. Bambergs K. Ģeoloģija un hidroģeoloģija. Rīga: Zvaigzne, 1993.
7. Biotopu rokasgrāmata. Rīga: Preses nams, 2000.
8. Civilā aizsardzība. Minimālās prasības civilās aizsardzības kursa saturam vispārējā un profesionālajā izglītībā. Prezentācija [skatīts 2020. gada 10.martā]. Pieejams: *https://visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/civila_aizsardziba.pdf*

9. Civilās aizsardzības un katastrofas pārvaldīšanas likums [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/282333-civilas-aizsardzibas-un-katastrofas-parvaldisanas-likums*
10. Clapham W. B., JR. Natural ecosystems. New York: Macmillan Publishing Co., Inc.,1993.
11. Darba aizsardzības apmācību metodes. – Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Darba_aizsardzibas_apmacibas_metodes.pdf*
12. Darba aizsardzības likums [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=26020*
13. Darba devēja rokasgrāmata. – Rīga: Latvijas Darba devēju konfederācija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://www.lm.gov.lv/upload/darba_devejiem/darb_dev_rok.pdf*
14. Darba drošība. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/12/Darba_drosiba.pdf*
15. Latvijas iedzīvotāju medikamentu lietošanas paradumi saaukstēšanās slimību gadījumos [skatīts 2020. gada 10.martā]. Pieejams: *http://www.veselibasprojekti.lv/upload/raksti/Pilna_petijuma_analize26032010.pdf*
16. Latvijas jaunatnes padome. Kā atpazīt viltus ziņas. [skatīts 2020. gada 10.martā]. Pieejams: *http://ljp.lv/index.php/ka-atpazit-viltus-zinas*
17. Latvijas Republikas likums "Par īpaši aizsargājamām dabas teritorijām" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=59994*
18. Latvijas Republikas Trešais nacionālais ziņojums ANO Vispārējās konvencijas par klimata pārmaiņām ietvaros. Rīga: Vides projekti, 2001.
19. Latvijas vides, ģeoloģijas un meteoroloģijas centra tīmekļa vietne. Vide. [skatīts 2020. gada 10.martā]. Pieejams: https://www.meteo.lv/lapas/vide/vide?id=1134&nid=320
20. Ministru kabineta 2017. gada 5. decembra noteikumi Nr. 716 "Minimālās prasības obligātā civilās aizsardzības kursa saturam un nodarbināto civilās aizsardzības apmācības saturam" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/295896-minimalas-prasibas-obligata-civilas-aizsardzibas-kursa-saturam-un-nodarbinato-civilas-aizsardzibas-apmacibas-saturam-*
21. Ministru kabineta 2016. gada 19. aprīļa noteikumi Nr. 238 "Ugunsdrošības noteikumi" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/281646-ugunsdrosibas- noteikumi*
22. Ministru kabineta 2010. gada 10. augusta noteikumi Nr. 749 "Apmācības kārtība darba aizsardzības jautājumos" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=214922*
23. Ministru kabineta 2008. gada 25. marta noteikumi Nr. 195 "Mašīnu drošības noteikumi" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=173016*
24. Ministru kabineta 2009. gada 10. marta noteikumi Nr. 219 "Kārtība, kādā veicama obligātā veselības pārbaude" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=189070*
25. Ministru kabineta 2007. gada 2. oktobra noteikumi Nr. 660 "Darba vides iekšējās uzraudzības veikšanas kārtība" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=164271*
26. Ministru kabineta 2007. gada 28. augusta noteikumi Nr. 568 "Kārtība, kādā noformējams administratīvā pārkāpuma protokols-paziņojums par mehānisko transportlīdzekļu pārvietošanās noteikumu pārkāpšanu ārpus autoceļiem Baltijas jūras un Rīgas jūras līča piekrastes krasta kāpu aizsargjoslā, pludmalē vai īpaši aizsargājamā dabas teritorijā" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/ta/id/163021-kartiba-kada-noformejams-administrativa-parkapuma-protokols-pazinojums-par-mehanisko-transportlidzeklu-parvietosanas*
27. Ministru kabineta 2002. gada 9. decembra noteikumi Nr. 526 "Darba aizsardzības prasības, lietojot darba aprīkojumu un strādājot augstumā" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=69282&version_date=02.06.2007&from=off*

28. Ministru kabineta 2002. gada 17. septembra noteikumi Nr. 427 "Uzticības personu ievēlēšanas un darbības kārtība" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=66827*
29. Ministru kabineta 2002. gada 3. septembra noteikumi Nr. 400 "Darba aizsardzības prasības drošības zīmju lietošanā" [skatīts 2020. gada 10.martā]. Pieejams: *http://www.likumi.lv/doc.php?id=66071*
30. Ministru kabineta 2002. gada 20. augusta noteikumi Nr. 372 "Darba aizsardzības prasības, lietojot individuālos aizsardzības līdzekļus" [skatīts 2020. gada 10.martā]. Pieejams: *https://likumi.lv/doc.php?id=65619*
31. NAPO filmas [skatīts 2020. gada 10.martā]. Pieejams: *https://www.napofilm.net/lv/napos-films/films?page=1&view_mode=page_grid*
32. Neatliekamās medicīniskās palīdzības dienesta tīmekļa vietne. Informatīvie materiāli. [skatīts 2020. gada 10.martā]. Pieejams: *http://www.nmpd.gov.lv/nmpd/medijiem/*
33. Pastors A. Baltijas jūras piekraste un Rīgas jūras līcis. Latvijas ģeogrāfija. Rīga: Zinātne, 1997.
34. Plakāts mīts "Darba aizsardzība ir tikai darba devēja uzdevums" [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/darba-aizsardziba-ir-lieki-izdevumi.pdf*
35. Plakāts mīts "Darba aizsardzība ir tikai lieki izdevumi" [skatīts 2020. gada 10.martā]. Pieejams: *http://osha.lv/lv/publications/files/darba-aizsardziba-ir-lieki-izdevumi.pdf*
36. Plakāts "Nepaej garām – ziņo par riskiem darba vietā!" [skatīts 2020. gada 10.martā]. Pieejams: *http://stradavesels.lv/Uploads/2014/02/11/15_2010_Plakats_A2_Zino_par_riskiem_final.pdf*
37. Psihosociālā darba vide. Rīga: Latvijas Brīvo arodbiedrību savienība, Labklājības ministrija, 2010 [skatīts 2020. gada 10.martā]. Pieejams: http://stradavesels.lv/Uploads/2014/02/12/psihosocialadarbavide.pdf
38. Skolas vecuma bērnu un pusaudžu veselība [skatīts 2020. gada 10.martā]. Pieejams: *https://spkc.gov.lv/upload/Petijumi%20un%20zinojumi/Sabiedribas%20veselibas%20petijumi/skolas_vecuma_bernu_un_pusaudzu_veseliba_svs_4merka_izvertejums_2008.pdf*

MODUĻA Informācijas un komunikācijas tehnoloģijas (1.līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas: 1) apgūt un lietot dažādas ikdienas lietotnes, lai paaugstinātu mācību un darba produktivitāti; 2) iedziļināties informācijas sistēmu un tiešsaistes rīku dažādībā un lietošanas apguvē, lai nostiprinātu digitālās prasmes un izvēlētos atbilstošāko risinājumu ikdienišķās problēmsituācijās; 3) ievērot intelektuālā īpašuma tiesības un rīkoties atbildīgi digitālo tehnoloģiju izmantošanas procesā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Ievērot normatīvo aktu prasības, kas nodrošina drošu informācijas tehnoloģiju lietošanu un informācijas apriti. 2. Lietot datortīklus un izplatītākās programmatūras datu ieguvei un apstrādei. 3. Pamatoti izvēlēties, pielāgot un lietot piemērotākos saziņas, informācijas ieguves un apmaiņas rīkus darba uzdevumu izpildei un profesionālai pilnveidei.
Moduļa ieejas nosacījumi	Apgūta vispārējās pamatizglītības programma.
Moduļa apguves novērtēšana	Izglītojamo sasniegumus vērtē 10 ballu vērtēšanas skalā, vērtējot iegūto zināšanu apjomu, kvalitāti, apgūtās pamatprasmes mācību jomā un caurviju prasmes, attīstītos ieradumus un attieksmes, kas apliecina vērtības un tikumus un mācību sasniegumu attīstības dinamiku. Noslēgumā izglītojamais izstrādā ar nozari vai ikdienas situācijām saistītu projektu, analizējot savus un citu paradumus un ikdienas izvēles. Projekta izstrādē ir ievērojami šādi nosacījumi: 1. Konkrētā uzdevuma veikšanai ir jāizmanto dažādas drošas detalizētas informācijas meklēšanas stratēģijas, vienkāršas datu vākšanas metodes, saziņas tīkli, sadarbības rīki un tiešsaistes pakalpojumi, pamatojot savu izvēli. 2. Iegūtie dati attēlojami prezentācijā, ievērojot informācijas atlases, attēlošanas un strukturēšanas pamatprincipus. 3. Prezentācijā iekļautie digitālie attēli, audio un video datnes izmantojami un apstrādājami atbilstoši mērķim. 4. Prezentācijā iekļaujami resursu (laika, finanšu, materiālu, tehnoloģiju un cilvēkresursu) pārvaldības risinājumu piemēri nozarē, to analīze, stiprās puses un iespējas. 5. Projekta izstrādē un lietošanā ir ievērojami programmatūras licences nosacījumi, intelektuālā īpašuma un personas datu aizsardzība.
Moduļa nozīme un vieta kartē	Īsteno kā mūžizglītības moduli, ja netiek īstenots informātikas pamatkurss vai tehnoloģiju mācību jomā – datorika, dizains un tehnoloģija un programmēšana.

MODUĻA Informācijas un komunikācijas tehnoloģijas (1.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: ievērot normatīvo aktu prasības, kas nodrošina drošu informācijas tehnoloģiju lietošanu un informācijas apriti. Zina: faktorus, kas var ietekmēt un apdraudēt cilvēka fizisko un garīgo veselību, drošības riskus, lietojot atvērtu datu apmaiņu, un vides ilgtspējības un ētiskos apsvērumus. Izprot: drošas informācijas aprites nepieciešamību un drošas darba vides nozīmi veselības saglabāšanai.	10% no moduļa kopējā apjoma	Raksturo nozīmīgākos noteikumus programmatūras un lietotāja licenču, intelektuālā īpašuma un personas datu aizsardzībai.	Izskaidro un izmanto juridiskos aspektus un nozīmīgākos noteikumus programmatūras un lietotāja licenču, intelektuālā īpašuma un personas datu aizsardzībai.
		Uzskaita būtiskos faktorus, kas var ietekmēt un apdraudēt cilvēka fizisko un garīgo veselību, un piedāvā dažus pasākumus, kā izvairīties no apdraudējumiem un atkarībām.	Novērtē un analizē faktorus, kas var ietekmēt un apdraudēt cilvēka fizisko un garīgo veselību, un veic pasākumus, lai izvairītos no apdraudējumiem un atkarībām.
		Piedāvā iespējamos variantus, kāda ir ergonomikas prasībām un darba uzdevumam atbilstoša darba vieta.	Analizē savas darba vietas atbilstību ergonomikas prasībām un iekārto to atbilstoši šīm prasībām un veicamajam darba uzdevumam.
		Raksturo lielākos drošības riskus, veicot datu apmaiņu, un aizsardzības līdzekļu izvēles principus, skaidro dotā uzdevuma veikšanai nepieciešamo tehnoloģiju un veicamo darbību ietekmi uz lietotāju veselību un vidi.	Izskaidro iespējamos drošības riskus atvērtas datu apmaiņas laikā un salīdzina atvērtas un šifrētas datu apmaiņas priekšrocības un trūkumus, un ievēro darba drošības prasības atbilstoši situācijai un apdraudējumam, kā arī skaidro uzdevuma veikšanai nepieciešamo tehnoloģiju un veicamo darbību ietekmi.
2. Spēj: lietot datortīklus un izplatītākās lietotnes datu ieguvei un apstrādei. Zina: biežāk lietotos datortīkla veidus un risinājumus, programmatūras dzīves cikla galvenos posmus. Izprot: datortīklu un izplatītāko lietotņu lietošanas	65% no moduļa kopējā apjoma	Raksturo ar piemēriem biežāk lietotos datortīkla veidus un drošības risinājumus, dažādas programmvadāmas ierīces un to izmantojumu sadzīvē un ražošanā.	Analizē dažādus datortīkla uzbūves principus, drošības risinājumus un piedāvā lietošanas iespējas atbilstoši lietotāja vajadzībām un drošības apsvērumiem, tai skaitā to sadzīvē un ražošanā.
		Raksturo biežāk izplatītās operētājsistēmas, to priekšrocības, trūkumus un iespējas darbam ar dažādām programmvadāmajām ierīcēm.	Izstrādā programmvadāmo ierīču komplektāciju un dokumentāciju atbilstoši lietotāja vajadzībām, piemērojot atbilstošus tehniskos parametrus nepieciešamajai funkcionalitātei, tai skaitā datorvadāmās iekārtas datorizētu telpisku modeļu, digitālu rasējumu un attēlu izveidē.

nozīmi drošā datu ieguvē un apstrādē.		Piedāvā dažādas dokumentu koplietošanas iespējas. Izmantojot datu analīzes lietotnes, sagatavo un organizē mērķauditorijas aptaujas un anketēšanas formas.	Izvērtē un izmanto dažādas dokumentu koplietošanas iespējas, nosakot atšķirīgiem lietotājiem atšķirīgas tiesības un iespējas. Veic savas aptaujas iegūto datu manuālu un automatizētu apstrādi.
		Veido un demonstrē prezentācijas, ievērojot informācijas attēlošanas pamatprincipus, atbilstoši mērķauditorijai un pieejamajam tehniskajam aprīkojumam.	Izveido un demonstrē prezentācijas, ievērojot informācijas atlases un strukturēšanas pamatprincipus, izvērtējot mērķauditorijas specifiku, pieejamo tehnisko aprīkojumu. Ievēro IT drošības, autortiesību un personas datu aizsardzības prasības.
3. Spēj: pamatoti izvēlēties, pielāgot un lietot piemērotākos saziņas, informācijas ieguves un apmaiņas rīkus darba uzdevumu izpildei un profesionālai pilnveidei. Zina: dažādus saziņas, informācijas ieguves un apmaiņas rīkus, pētniecības metodes. Izprot: atbilstošu rīku izvēles nozīmi informācijas ieguvei, apstrādei un saziņai un efektīvu rezultātu ieguvei.	25% no moduļa kopējā apjoma	Izvēlas piemērotākos saziņas, informācijas ieguves un apmaiņas rīkus un interneta pakalpojumus, kas paredzēti produktivitātes pilnveidošanai un mācību uzdevumu veikšanai.	Izvēlas, pielāgo un lieto piemērotākos saziņas, informācijas ieguves un apmaiņas rīkus un citus interneta pakalpojumus, pilnveidojot produktivitāti mācību uzdevumu veikšanai.
		Noskaidro lietotāju paradumus, intereses un to, kādus risinājumus un kā ikdienā izmanto, lietojot dažādas pētniecības metodes.	Pēta un analizē savus un citu ikdienas paradumus, intereses un ikdienas izvēles, izmantojot dažādas pētniecības metodes, reflektē par iespējām nākotnē savā nozarē.
		Raksturo mākoņprogrammas, konta izmantošanas iespējas, izmanto vienkāršas lietotnes un tiešsaistes komunikācijas platformas, un vismaz divus informācijas tehnoloģijas nodrošinātus epakalpojumus, pieprasot vai saņemot tos attālinātā veidā.	Izveido un uzglabā savus datus mākoņprogrammā, plaši lieto sava e-pasta konta izmantošanas iespējas, brīvi lieto informācijas tehnoloģijas nodrošinātus epakalpojumus, izvēlas situācijai piemērotāko un pamato savu izvēli.

Izmantojamie avoti:

1. Aizpuriete V. Datorzinības. – Ozolnieki, 2002.
2. Aizpuriete V. *Microsoft Excel* profesionālai izglītībai. Rīga: Mācību grāmata, 2002.
3. Akadēmiskā terminu datubāze [skatīts 2020. gada 23. aprīlī]. Pieejams*: http://termini.lza.lv/term.php*
4. Centrālās statistikas pārvalde. Zinātne un IKT, datoru lietošanas paradumi [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://www.csb.gov.lv/lv/statistika/statistikas-temas/zinatne-ikt/datori-internets*
5. Dažādu nozaru enciklopēdijas [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://llufb.llu.lv/lv/datubazes-un-katalogi*
6. Digitālās prasmes [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://europass.cedefop.europa.eu/lv/resources/digital-competences*
7. Drošs internets. Projekta materiāli darbam [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://drossinternets.lv/lv/materials*
8. Dukulis I. Apgūsim jauno *Word! Microsoft Office Word 2003*. – Rīga: Turība, 2005.

9. Dukulis I. Aprēķini un datu grafiskais attēlojums. Programma *Microsoft Excel 2000*. – Rīga: Turība, 2002.
10. Dukulis I., Gultniece I., Ivane A., Krišjānis P., Mazurs R., Veiss K., Vēzis V. Informātika. Materiāls izstrādāts ESF darbības programmas 2007.–2013. gadam "Cilvēkresursi un nodarbinātība" 1.2. prioritātes "Izglītība un prasmes" 1.2.1. pasākuma "Profesionālās izglītības un vispārējo prasmju attīstība" 1.2.1.2. aktivitātes "Vispārējo zināšanu un prasmju uzlabošana" 1.2.1.1.2. apakšaktivitātē "Profesionālajā izglītībā iesaistīto pedagogu kompetences paaugstināšana" Latvijas Universitātes realizētajā projektā "Profesionālajā izglītībā iesaistīto vispārizglītojošo mācību priekšmetu pedagogu kompetences paaugstināšana", Rīga, 2011 [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://profizgl.lu.lv/course/view.php?id=5*
11. Eiropas datorprasmes sertifikāts [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.ecdl.lv/*
12. FOLDOC – tiešsaistes vārdnīca visās datorzinātņu jomās [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://foldoc.org/*
13. Internetresurss: mācību iespējas, resursi, materiāli skolotājiem [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://csedweek.org/*
14. InterOperability Laboratory – mācību dokumenti un kursi [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.iol.unh.edu/education/training/*
15. IT programmatūras lietojums elektroenerģētikā [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Informaciju_tehnologiju_programmaturu_pielietojums_elektroenergetika2.pdf*
16. Journal of Information Technology in Construction – brīvpieejas žurnāls (1996–2020) [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.itcon.org/*
17. Kamars A. Tīmekļa lapu veidošana HTML un CSS. E-grāmata. – Zvaigzne ABC [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.zvaigzne.lv/lv/gramatas/apraksts/102205-timekla_lapu_veidosana_html_un_css.html*
18. Katalogi un datubāzes [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://lnb.lv/lv/katalogi-un-datubazes*
19. Kliedere I. Lietišķā informātika. Mācību līdzeklis, papild. izd. Rīga: Juridiskā koledža, 2008.
20. Learnthat – bezmaksas mācības un tiešsaistes kursi [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://learnthat.com/*
21. Latvijas Nacionālais terminoloģijas portāls [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://termini.gov.lv/*
22. LIIS mācību materiāli [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.sakaru-pasaule.lv/main.php3?sub=view&RID=582*
23. Mācību resursu krātuve. [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://skola2030.lv/lv/atbalsts/atbalsts-istenosanai/macibu-resursu-kratuve*
24. Pamatkompetences mūžizglītības kontekstā [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://data.consilium.europa.eu/doc/document/ST-5464-2018-ADD-2/EN/pdf*
25. Poriķe J., Dumpe D. Digitālās prasmes darba vajadzībām [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Digitalas_prasmes_darba_vajadzibam.pdf*
26. Resursi pedagogiem IKT izmantošanai, apguvei [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.ourict.co.uk/teaching-computer-science/*
27. Saziņa 21. gadsimtā – digitāli kompetents pilsonis [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Sazina_21gs_digitali_kompetents_pilsonis2.pdf*
28. Scandinavian Journal of Information Systems – brīvpieejas žurnāls (1989– 2019) [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://iris.cs.aau.dk/index.php/archieve.html*
29. Valsts darba inspekcijas materiāls. Ergonomikas jautājumi, darba vietas iekārtojums [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.vdi.gov.lv/files/darbs_ar_datoru.pdf*
30. Veiss K. Informātika vidusskolai. Mācību grāmata (tai skaitā e-grāmata). – Rīga: Zvaigzne ABC, 2007. Sagataves e-grāmata [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.zvaigzne.lv/lv/gramatas/apraksts/92489-informatika_vidusskola_sagataves_-_bezmaksas.html*

31. Veiss K. Informātika vidusskolā. Skolotāja grāmata. – Rīga: Zvaigzne ABC, 2009.
32. Vilde V. Informātika pamatskolai. Skolotāja grāmata, 1.–6. daļa. Rīga: RaKa, 2008.
33. Whatis.com – vadošā IT enciklopēdija un mācību centrs [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://whatis.techtarget.com/*

MODUĻA Informācijas un komunikācijas tehnoloģijas (2.līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas 1) apgūt un lietot dažādas ikdienas lietotnes, lai paaugstinātu sava mācību un personiskā darba produktivitāti; 2) iedziļināties informācijas sistēmu un tiešsaistes rīku dažādībā un lietošanas apguvē, lai nostiprinātu digitālās prasmes un izvēlētos atbilstošāko risinājumu ikdienišķās problēmsituācijās; 3) ievērot intelektuālā īpašuma tiesības un rīkoties atbildīgi digitālo tehnoloģiju izmantošanas procesā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1.Veidot digitālo saturu atbilstoši profesionālās darbības specifikai, ņemot vērā iespējamos drošības riskus. 2.Atpazīt un analizēt informācijas dizaina risinājumus, to izstrādes tehnoloģiskos procesus un ietekmi uz lietotāju. 3. Lietot informācijas un komunikācijas tehnoloģijas profesionālajā darbā, ievērojot programmatūras licences nosacījumus, intelektuālā īpašuma un personas datu aizsardzību.
Moduļa ieejas nosacījumi	Apgūts modulis "Informācijas un komunikācijas tehnoloģijas (1. līmenis)".
Moduļa apguves novērtēšana	Izglītojamo sasniegumus vērtē 10 ballu vērtēšanas skalā, vērtējot iegūto zināšanu apjomu, kvalitāti, apgūtās pamatprasmes mācību jomā un caurviju prasmes, attīstītos ieradumus un attieksmi, kas apliecina vērtības un tikumus un mācību sasniegumu attīstības dinamiku. Noslēgumā izglītojamais izstrādā ar nozari saistītu projektu, kurā nepieciešams lietot dažādas lietotnes, kas paaugstina darba produktivitāti un nostiprina digitālās prasmes. Projekta izstrādē ir ievērojami šādi nosacījumi: 1. Jāanalizē nozares dizaina risinājumi, to izstrādes tehnoloģiskie procesi, jāizvērtē izmantotie materiāli, tehnoloģiskie procesi, to priekšrocības un trūkumi, jāsalīdzina to ietekme uz lietotāju veselību un vidi. 2.Jālieto droši un piemēroti saziņas, informācijas ieguves un apmaiņas rīki un citi interneta pakalpojumi, pamatojot savu izvēli. 3.Veidojot digitālo saturu, jāievēro informācijas atlases, attēlošanas un strukturēšanas pamatprincipi, programmatūras licences nosacījumi, intelektuālā īpašuma un personas datu aizsardzība. 4.Digitālie attēli, audio un video datnes izmantojami un apstrādājami atbilstoši mērķim. 5. Jāpiedāvā atbilstošākais risinājums, apskatot piedāvāto digitālo risinājumu problēmsituācijai darba dzīvē.
Moduļa nozīme un vieta kartē	Īsteno kā mūžizglītības moduli, ja netiek īstenots informātikas pamatkurss vai tehnoloģiju mācību jomā – datorika, dizains un tehnoloģija un programmēšana.

MODUĻA Informācijas un komunikācijas tehnoloģijas (2.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: veidot digitālo saturu atbilstoši profesionālās darbības specifikai, ievērojot iespējamos drošības riskus. Zina: strukturētu dokumentu un izklājlapu veidošanas principus, digitālo attēlu, audio un video datņu apstrādes principus, datu analīzes metodes, datubāzes atbilstoši to mērķiem, tēmai, saturam, auditorijai un tehnoloģijām. Izprot: digitālā satura radīšanas nozīmi profesionālās darbības nodrošināšanai, ievērojot informācijas tehnoloģiju drošības un personas datu aizsardzības prasības	50% no moduļa kopējā apjoma	Nosauc un raksturo ar piemēriem programmatūras dzīves cikla posmus, ikdienas darba procesus, atpazīst automatizācijai piemērotas daļas ikdienas darba procesos un plāno to automatizāciju.	Analizē programmatūras dzīves cikla galvenos posmus, t.sk. specificēšanu, projektēšanu, izstrādi, testēšanu, uzturēšanu, un piedāvā automatizācijai piemērotas daļas ikdienas darba procesos un analizē to automatizācijas iespējas.
		Sagatavo un rediģē ar palīdzību strukturētus dokumentus, iekļaujot dažādus objektus un izmantojot darba efektivitātes un automatizācijas rīkus un izklājlapas, veic nepieciešamos aprēķinus.	Patstāvīgi sagatavo, rediģē un formatē lielus, strukturētus dokumentus, iekļaujot dažādus objektus un izklājlapas, izmanto lietotņu darba efektivitātes un automatizācijas rīkus, veic datu atlasi un aprēķinus atbilstoši kritērijiem, kā arī ievades un formulu validāciju atbilstoši lietotāja datu apstrādes vajadzībām un savam izvēlētajam risinājumam.
		Izmanto datu analīzes lietotnes mācību procesā iegūto datu strukturēšanai.	Patstāvīgi veido savu risinājumu mācību procesā iegūto datu strukturēšanai un attēlošanai atbilstoši grafikas dizaina noformējuma pamatprincipiem, izmantojot datu analīzes automatizācijas un vizualizācijas lietotnes.
		Veido un apstrādā digitālus attēlus, audio un video datnes un raksturo praktiskus tehnoloģiskos risinājumus datorizētu telpisku modeļu, digitālu rasējumu un attēlu izveidei.	Veido un apstrādā digitālus attēlus, audio un video datnes, izvēloties lietotnes atbilstoši dotajam uzdevumam, un salīdzina dažādus praktiskus tehnoloģiskos risinājumus datorizētu telpisku modeļu, digitālu rasējumu un attēlu izveidei, ievērojot informāciju par darba apstākļu ietekmi uz lietotāju veselību un vidi.
		Skaidro pamatjēdzienus un veic datu izguvi un apstrādi no publiski pieejamām datubāzēm, nosauc nozares specializētās datubāzes.	Patstāvīgi veido datubāzes, novēršot datu dublēšanos, un veic datu izguvi un pēcapstrādi no publiski pieejamām un specializētajām datubāzēm atbilstoši nozares specifikai.

2. Spēj: atpazīt un analizēt informācijas dizaina risinājumus, to izstrādes tehnoloģiskos procesus, to ietekmi uz lietotāju. Zina: mediju veidus, medijpratības principus, informācijas ticamības kritērijus, informācijas dizaina procesu, iesaistītos darbiniekus, to lomas, uzdevumus. Izprot: informācijas dizaina risinājumu sniegtās iespējas mūsdienīgas saziņas veidošanā.	25% no moduļa kopējā apjoma	Atrod informāciju medijos atbilstoši dotajam uzdevumam. Raksturo vismaz divos medijos izmantotus informācijas dizaina risinājumus, analizē konkrēto piemēru priekšrocības un trūkumus, nosaka, dizaina risinājuma iesaistīto darbinieku lomu risinājumu izstrādes procesā.	Atrod informāciju dažādos medijos atbilstoši izvirzītajam mērķim. Salīdzina un analizē medijos izmantotos informācijas dizaina risinājumus, to priekšrocības un trūkumus un iesaistīto darbinieku lomu dizaina risinājumu izstrādes procesā, reflektē par savām prasmēm un profesionālajām interesēm.
		Plāno informācijas dizaina risinājumus, veido dažādus modeļus un variantus, testē tos un piedāvā ierosinājumus izstrādes darba plāna pilnveidei.	Plānojot informācijas dizaina risinājumu, veido dažādus modeļus un variantus, testē un lieto radīto risinājumu iterācijas, analizē iegūtos datus un formulē pamatotus ierosinājumus izstrādes darba plāna pilnveidei.
3. Spēj: lietot informācijas un komunikācijas tehnoloģijas profesionālajā darbā, ievērojot programmatūras licences nosacījumus, intelektuālā īpašuma un personas datu aizsardzību. Zina: nozares specializētās datorprogrammas, to izmantošanas iespējas un nosacījumus. Izprot: nozares specializēto datorprogrammu un saziņas, informācijas ieguves un apmaiņas rīku un citu interneta pakalpojumu lietošanas nepieciešamību un piemērotību profesionālajā darbībā.	25% no moduļa kopējā apjoma	Klasificē nozares specializētās datorprogrammas, raksturo to darbības pamatprincipus un apraksta to izmantošanas iespējas. Profesionālajā darbībā lieto specializētās datorprogrammas un piemērotus saziņas, informācijas ieguves un apmaiņas rīkus un citus interneta pakalpojumus, ievērojot īpašuma tiesību un personu datu aizsardzības nosacījumus.	Analizē nozares specializētās datorprogrammas, izvērtē to darbības pamatprincipus un izmantošanas iespējas. Izvēlas, pielāgo atbilstoši situācijai un profesionālajā darbībā lieto specializētās datorprogrammas un piemērotus saziņas, informācijas ieguves un apmaiņas rīkus un citus interneta pakalpojumus, ievērojot īpašuma tiesību un personu datu aizsardzības nosacījumus.

Izmantojamie avoti:

1. Aizpuriete V. Datorzinības. – Ozolnieki, 2002.
2. Aizpuriete V. *Microsoft Excel* profesionālai izglītībai. Rīga: Mācību grāmata, 2002.
3. Akadēmiskā terminu datubāze [skatīts 2020. gada 23. aprīlī]. Pieejams*: http://termini.lza.lv/term.php*
4. Centrālās statistikas pārvalde. Zinātne un IKT, datoru lietošanas paradumi [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://www.csb.gov.lv/lv/statistika/statistikas-temas/zinatne-ikt/datori-internets*
5. Dažādu nozaru enciklopēdijas [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://llufb.llu.lv/lv/datubazes-un-katalogi*
6. Digitālās prasmes [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://europass.cedefop.europa.eu/lv/resources/digital-competences*
7. Drošs internets. Projekta materiāli darbam [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://drossinternets.lv/lv/materials*
8. Dukulis I. Apgūsim jauno *Word! Microsoft Office Word 2003*. – Rīga: Turība, 2005.
9. Dukulis I. Aprēķini un datu grafiskais attēlojums. Programma *Microsoft Excel 2000*. – Rīga: Turība, 2002.
10. Dukulis I., Gultniece I., Ivane A., Krišjānis P., Mazurs R., Veiss K., Vēzis V. Informātika. Materiāls izstrādāts ESF darbības programmas 2007.–2013. gadam "Cilvēkresursi un nodarbinātība" 1.2. prioritātes "Izglītība un prasmes" 1.2.1. pasākuma "Profesionālās izglītības un vispārējo prasmju attīstība" 1.2.1.2. aktivitātes "Vispārējo zināšanu un prasmju uzlabošana" 1.2.1.1.2. apakšaktivitātē "Profesionālajā izglītībā iesaistīto pedagogu kompetences paaugstināšana" Latvijas Universitātes realizētajā projektā "Profesionālajā izglītībā iesaistīto vispārizglītojošo mācību priekšmetu pedagogu kompetences paaugstināšana", Rīga, 2011 [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://profizgl.lu.lv/course/view.php?id=5*
11. Eiropas datorprasmes sertifikāts [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.ecdl.lv/*
12. FOLDOC – tiešsaistes vārdnīca visās datorzinātņu jomās [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://foldoc.org/*
13. Internetresurss: mācību iespējas, resursi, materiāli skolotājiem [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://csedweek.org/*
14. InterOperability Laboratory – mācību dokumenti un kursi [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.iol.unh.edu/education/training/*
15. IT programmatūras lietojums elektroenerģētikā [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Informaciju_tehnologiju_programmaturu_pielietojums_elektroenergetika2.pdf*
16. Journal of Information Technology in Construction – brīvpieejas žurnāls (1996–2020) [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.itcon.org/*
17. Kamars A. Tīmekļa lapu veidošana HTML un CSS. E-grāmata. – Zvaigzne ABC [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.zvaigzne.lv/lv/gramatas/apraksts/102205-timekla_lapu_veidosana_html_un_css.html*
18. Katalogi un datubāzes [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://lnb.lv/lv/katalogi-un-datubazes*
19. Kliedere I. Lietišķā informātika. Mācību līdzeklis, papild. izd. Rīga: Juridiskā koledža, 2008.
20. Learnthat – bezmaksas mācības un tiešsaistes kursi [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://learnthat.com/*
21. Latvijas Nacionālais terminoloģijas portāls [skatīts 2020. gada 23. aprīlī]. Pieejams: *https://termini.gov.lv/*
22. LIIS mācību materiāli [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.sakaru-pasaule.lv/main.php3?sub=view&RID=582*
23. Mācību resursu krātuve. [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://skola2030.lv/lv/atbalsts/atbalsts-istenosanai/macibu-resursu-kratuve*
24. Pamatkompetences mūžizglītības kontekstā [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://data.consilium.europa.eu/doc/document/ST-5464-2018-ADD-2/EN/pdf*

25. Poriķe J., Dumpe D. Digitālās prasmes darba vajadzībām [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Digitalas_prasmes_darba_vajadzibam.pdf*
26. Resursi pedagogiem IKT izmantošanai, apguvei [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.ourict.co.uk/teaching-computer-science/*
27. Saziņa 21. gadsimtā – digitāli kompetents pilsonis [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.muzizglitiba.lv/sites/default/files/Sazina_21gs_digitali_kompetents_pilsonis2.pdf*
28. Scandinavian Journal of Information Systems – brīvpieejas žurnāls (1989– 2019) [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://iris.cs.aau.dk/index.php/archieve.html*
29. Valsts darba inspekcijas materiāls. Ergonomikas jautājumi, darba vietas iekārtojums [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.vdi.gov.lv/files/darbs_ar_datoru.pdf*
30. Veiss K. Informātika vidusskolai. Mācību grāmata (tai skaitā e-grāmata). – Rīga: Zvaigzne ABC, 2007. Sagataves e-grāmata [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://www.zvaigzne.lv/lv/gramatas/apraksts/92489-informatika_vidusskola_sagataves_-_bezmaksas.html*
31. Veiss K. Informātika vidusskolā. Skolotāja grāmata. – Rīga: Zvaigzne ABC, 2009.
32. Vilde V. Informātika pamatskolai. Skolotāja grāmata, 1.–6. daļa. Rīga: RaKa, 2008.
33. Whatis.com – vadošā IT enciklopēdija un mācību centrs [skatīts 2020. gada 23. aprīlī]. Pieejams: *http://whatis.techtarget.com/*

MODUĻA Valodas, kultūras izpratne un izpausmes (1.līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas, izraisot interesi un zinātkāri par valodām un starpkultūru saziņu, pilnveidojot izglītojamo zināšanas un izpratni par vietējo, valsts un Eiropas kultūras mantojumu un tā vietu pasaulē, veicinot izpratni par valodas un kultūras daudzveidību, nodrošinot profesionālās terminoloģijas apguvi svešvalodā(-s) izvēlētajā nozarē/sektorā un izglītojamo iespējas realizēt starptautiskās mobilitātes aktivitātes profesionālajā jomā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Novērtēt kultūru kā vērtību. 2. Lietot atbilstošo nozares/sektora profesionālās leksikas krājumu. 3. Pilnveidot valodas prasmes, noteikt tālākos mācību mērķus. 4. Raksturot nacionālās kultūras vērtības kā sistēmu un identifikācijas pamatu. 5. Toleranti veidot attiecības ar dažādu kultūru un subkultūru, reliģiju un dzimumu pārstāvjiem, saglabājot savu nacionālo identitāti. 6. Skaidrot kultūras un mākslas izpausmes veidus.
Moduļa ieejas nosacījumi	Apgūta pamatizglītība
Moduļa apguves novērtēšana	Moduļa "Valodas, kultūras izpratne un izpausmes (1. līmenis)" apguves noslēgumā izglītojamie kārto pārbaudījumu – prezentē portfolio. Portfolio sadaļas: Plakāts/infografika u.c. par kultūras komponentiem. Argumentētā eseja, piemēram, "Kultūra – personības attīstības instruments un resurss". Profesionālo terminu vārdnīca ar skaidrojumiem un lietojuma piemēriem. Diskusijas "Valodu prasmes loma profesionālajā un personības pilnveidē" apkopojums. Europass CV. Motivācijas vēstule. Eiropas Valodu portfeļa daļas (Valodu pase, Valodu biogrāfija, valodu dosjē). Ieskats kādā subkultūrā. Ideju karte par kultūras formu daudzveidību, to vietu un nozīmi sabiedrības veidošanā, attīstībā, sadzīves un kultūras organizācijā. Gan pedagogs novērtē paveikto 10 ballu skalā, gan izglītojamie savstarpēji novērtē darbus, gan pats izglītojamais savu sniegumu izvērtē pašnovērtējumā pēc pedagoga sagatavotas pašnovērtējuma veidlapas ar vērtēšanas kritērijiem.
Moduļa nozīme un vieta kartē	Modulis iekļaujams profesionālās izglītības programmās 3. un 4. Latvijas kvalifikāciju ietvarstruktūras līmeņu profesionālās kvalifikācijas apguvei.

MODUĻA Valodas, kultūras izpratne un izpausmes (1.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: novērtēt kultūru kā vērtību. Zina: kultūras komponentus. Izprot: kultūru kā procesu, kurā iekļauta visa sabiedrība, un kultūras nozīmi personības attīstībā.	5% no moduļa kopējā apjoma	Identificē kultūras komponentus. Definē kultūru kā procesu, kurā iesaistīta visa sabiedrība. Nosauc un vispārīgi raksturo kultūras nozīmi personības attīstībā.	Raksturo un salīdzina kultūras komponentus. Ilustrē ar piemēriem kultūru kā procesu, kurā iesaistīta visa sabiedrība. Izskaidro ar vairākiem piemēriem kultūras nozīmi personības attīstībā.
2. Spēj: lietot atbilstošo nozares/sektora profesionālās leksikas krājumu. Zina: nozarē/sektorā lietoto terminoloģiju svešvalodā. Izprot: valodu prasmes nozīmīgumu profesionālajā un personības pilnveidē.	50% no moduļa kopējā apjoma	Ar vienkāršiem teikumiem apraksta svešvalodā profesijas mērķus un uzdevumus. Ar īsiem teikumiem veido vienkāršu aprakstu par darba procesā izmantojamajiem materiāliem/produktiem, iekārtām, darba instrumentiem, tehnoloģiskajiem procesiem. Apraksta valodu prasmes nozīmi karjeras veidošanā. Lieto svešvalodā terminoloģiju, kas saistīta ar profesiju. Uzdod jautājumus, uztver teksta galveno domu. Ar pedagoga palīdzību izveido Europass CV un motivācijas vēstuli.	Svešvalodā skaidri un detalizēti raksturo profesijas mērķus, uzdevumus un profesijas vietu nozarē. Veido detalizētus, sistēmiskus aprakstus un izklāstus par darba procesā izmantojamajiem materiāliem/produktiem iekārtām, darba instrumentiem, tehnoloģiskajiem procesiem. Novērtē valodu prasmes nozīmi karjeras veidošanā. Sazinās profesionālajā svešvalodā. Diskutē. Piedāvā problēmu risinājumu. Patstāvīgi izveido Europass CV un motivācijas vēstuli.
3. Spēj: pilnveidot valodas prasmes, noteikt tālākos mācību mērķus. Zina: jēdzienus Eiropas Valodu portfelis, Valodu pase, Valodu biogrāfija, dosjē, sociālie tīkli.	10% no moduļa kopējā apjoma	Definē jēdzienus Eiropas Valodu portfelis, Valodu pase, Valodu biogrāfija, dosjē, sociālie tīkli. Nosauc valodas apguves iespējas, izmantojot sociālos tīklus. Nosauc valodas prasmes līmeņu kritērijus.	Izveido Valodu pasi, Valodu biogrāfiju un dosjē. Izvērtē valodas apguves iespējas, izmantojot sociālos tīklus. Veic pašvērtējumu, lai noteiktu savu valodas prasmes līmeni.

Izprot: komunikācijas un kultūras savstarpējo saistību un komunikāciju kā kultūras aktivitāti.			
4. Spēj: raksturot nacionālās kultūras vērtības kā sistēmu un identifikācijas pamatu. Zina: jēdzienus vērtība, garīgās un materiālās vērtības, nacionālās un internacionālās vērtības, indivīda un sabiedrības vērtības, reliģija, tradīcijas, kultūras kanons. Izprot: kultūras kanona lomu un vērtību pasaules un Latvijas kultūrā	10% no moduļa kopējā apjoma	Izvērtē vērtību nozīmi savā dzīvē. Nosauc kopīgo un atšķirīgo rietumu un austrumu kultūrā. Identificē kultūras tradīciju veidošanās, saglabāšanas un pārmantojamības raksturu. Skaidro kultūru savstarpējo saistību, formu un elementu pārmantojamību, ietekmi pasaules un Latvijas kultūrā. Pamato nepieciešamību iesaistīties sabiedrības un kultūrvides veidošanas procesos. Nosauc izcilākos sasniegumus savā kultūrā.	Izvirza hipotēzi par vērtību nozīmi un lomu savā un sabiedrības dzīvē un pierāda to. Stiprina Latvijas kultūrtelpu kā sabiedrību saliedējošu pamatu un veicina tās popularizēšanu Eiropas un pasaules līmenī. Salīdzina un diskutē par tradīciju noturīgumu un mainību austrumu un rietumu kultūrā. Skaidro un raksturo tradīciju pārmantošanas iespējas un veidus tradicionālajā un mūsdienu kultūrā. Salīdzina pasaules un Latvijas kultūras informatīvos avotus un liecības. Sasaista vienotu vēsturisko vērtību apzināšanos ar savu piederību Latvijai. Ar vairākiem argumentiem izskaidro nepieciešamību iesaistīties sabiedrības un kultūrvides veidošanas procesos. Analizē iesaistīšanās virzienus. Novērtē un analizē izcilākos sasniegumus savā kultūrā.
5. Spēj: toleranti veidot attiecības ar dažādu kultūru un subkultūru, reliģiju un dzimumu pārstāvjiem, saglabājot savu nacionālo identitāti. Zina: jēdzienus popkultūra, subkultūra, kontrkultūra, hipiji, panki, goti, tolerance, globalizācija, kultūrdialogs, stereotipi, kultūras šoks. Izprot: sabiedrības lomu dažādu sabiedrības grupu	15% no moduļa kopējā apjoma	Identificē sabiedrības, dažādu sociālo grupu mijiedarbību un izpausmes kultūrtelpā. Paskaidro jēdzienu kontrkultūra. Identificē subkultūras pēc to pazīmēm. Raksturo savu nacionālo kultūridentitāti. Definē jēdzienu globalizācija. Definē jēdzienus stereotips un stereotipiskās domāšanas izpausmes. Raksturo kultūras šoka būtību, izpausmes radītājus un stadijas. Izskaidro tolerances jēdziena būtību un pamato nepieciešamību veidot pozitīvas attiecības ar dažādu kultūru un reliģiju pārstāvjiem.	Novērtē sabiedrības, dažādu sociālo grupu mijiedarbību un izpausmes kultūrtelpā. Novērtē kontrkultūras parādības sabiedrībā. Raksturo un analizē dažādas subkultūras, to izpausmes un liecības. Izvērtē un pamato savu vietu kultūrprocesu veidošanā. Salīdzina un raksturo globalizācijas izpausmes. Identificē stereotipiskās domāšanas veidu, analizē tā rašanās cēloņus. Analizē kultūras šoka rašanās cēloņus. Raksturo tolerances būtību, ilustrējot ar vairākiem piemēriem. Formulē

kultūras veidošanā un pastāvēšanā.		Nosauc idejas starpkultūru attiecību problēmu risināšanai.	secinājumus, kāpēc nepieciešams veidot pozitīvas attiecības ar dažādu kultūru, reliģiju un dzimumu pārstāvjiem. Analizē starpkultūru problēmu cēloņus, formulē ieteikumus starpkultūru komunikācijas veicināšanai.
6. Spēj: skaidrot kultūras un mākslas izpausmes veidus. Zina: mākslas veidus un moderno tehnoloģiju nozīmi kultūrā. Izprot: kultūras un mākslas formu daudzveidību, to vietu un nozīmi sabiedrības veidošanā, attīstībā, sadzīves un kultūras organizācijā.	10% no moduļa kopējā apjoma	Nosauc dažādas mākslas izpausmes formas. Nosauc nozīmīgākos mākslas stilus un virzienus. Nosauc ievērojamākās kultūras vērtības pasaules muzejos. Demonstrē faktu un ideju izpratni par kultūras formu lomu sabiedrības attīstībā, sadzīves un kultūras organizācijā.	Raksturo un salīdzina dažādās mākslas izpausmes formas. Raksturo nozīmīgākos mākslas stilus un virzienus. Raksturo un novērtē izcilākās kultūras vērtības pasaules muzejos. Novērtē un raksturo mākslas darbus un kultūras objektus to kultūrvēsturiskā kontekstā.

Izmantojamie avoti:

1. Agajevs V. Semiotika. – Rīga: Jumava, 2005.
2. Aldersons J. Mākslas un kultūras vārdnīca ar interneta atslēgvārdiem. – Rīga: Zvaigzne ABC, 2011.
3. Apele A. Prasme runāt publiski. – Rīga: Zvaigzne ABC, 2011.
4. Arnolda D. Saprast mākslu: sešas tēmas. – Rīga: Zvaigzne ABC, 2018.
5. Austruma S., Muižarāja I. Kulturoloģija vidusskolai. – Rīga: Zvaigzne ABC, 2005.
6. Austruma S., Muižarāja I. Kultūras vēsture. Metodiskais līdzeklis. – Rīga: ISEC, 2005.
7. Avotiņa A., Blūma D. u.c. Latvijas kultūras vēsture. – Rīga: Zvaigzne ABC, 2003.
8. Avotiņa A., Genese-Plaude I., Mūrnieks A., Pitkeviča I., Voitkāne I. Kulturoloģija kā integrējošs mācību kurss laikmetīgā mācību procesā. – Rīga: LU Pedagoģijas, psiholoģijas un mākslas fakultāte, 2013.
9. Baltijas ceļš [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.thebalticway.eu/*
10. Blūma D. Kultūras vēsture vārdos, jēdzienos un nosaukumos. – Rīga: RaKa, 2000.
11. Bodrijārs Ž. Simulakri un simulācija. – Rīga: Omnia mea, 2000.
12. Ceļā uz darbu [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://www.nva.gov.lv/karjera/docs/_52bcaaf265d237.51951269.pdf*
13. Dempsey A. Modernā māksla. – Rīga: Jāņa Rozes apgāds, 2018.
14. Duale Ausbildung – Rebecca wird Elektronikerin [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.pasch-net.de/de/pas/cls/sch/jus/sua/20933052.html*
15. Dubiņa I., Pērkone-Redoviča I. Literatūra un kino. XX gadsimts. Kultūras vēsture. – Rīga: Zvaigzne ABC, 2006.

16. Eiropas kopīgās pamatnostādnes valodas apguvei. Pašnovērtējuma tabula [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://europass.cedefop.europa.eu/sites/default/files/cefr-lv.pdf*
17. Eiropas literatūras vēsture: Hrestomātija. / Annikas Benuā-Dizosuā un Gija Fontēna redakcijā. – Rīga: Jāņa Rozes apgāds, 2013.
18. Eiropas Valodu portfelis (EVP). Principi un vadlīnijas ar paskaidrojumiem [skatīts 2019. gada 7. oktobrī]. Pieejams:
19. *https://valoda.lv/wp-content/uploads/docs/Projekti/LV_mat_evp.pdf*
20. Electrician [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.truity.com/career-profile/electrician*
21. EUROPASS [skatīts 2019. gada 22. maijā]. Pieejams: *http://europass.lv/*
22. Ērgle A., Purēns I., Sviestiņa I. Kulturoloģija. – Rīga: RaKa, 2009.
23. Filma "Latvijas valsts simboli" [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=brB8TrGpkVM*
24. Filma "Pūt, vējiņi. Latvijai 100". Smilšu kino [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=z3RsBKUT6xI*
25. Freids Z. Īgnums kultūrā. – Rīga: Zvaigzne ABC, 2000.
26. Herdera vārdnīca. Simboli. – Rīga: Pētergailis, 1994.
27. Hodža S., Teilors D. Māksla: enciklopēdija skolēniem. / Tulk. Rute Marta Jansone; red. Ilze Sausiņa. – Rīga: Zvaigzne ABC, 2018.
28. Ierosmes mācību priekšmeta "Kulturoloģija" apguvei. Metodiskais materiāls [skatīts 2019. gada 22. maijā]. Pieejams: *https://visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/kulturologija.pdf*
29. Ilustrētā arhitektūras vēsture. / Emīlijas Kolas redakcijā. – Rīga: Zvaigzne ABC, 2013.
30. Informācijas vide Latvijā: 21. gadsimta sākums. I. Brikšes redakcijā. – Rīga: Zinātne, 2006.
31. Islāms. – Rīga: Zvaigzne ABC, 2004.
32. Jermolajeva J., Jermolajevs V., Mūrnieks A. Kultūras vēsture. 20. gadsimts. – Rīga: RaKa, 2002.
33. Kagaine Z. Tēlainā domāšana vizuālajā mākslā. – Rīga: Zvaigzne ABC, 2005.
34. Kalniņa L., Zvirgzds J. Lielā simbolu enciklopēdija. – Rīga: Jumava, 2006.
35. Karasā F. P., Markadē I. Mākslas enciklopēdija. Glezniecības virzieni. – Rīga: Jumava, 2002.
36. Kasīrers E. Apcerējums par cilvēku. Ievads kultūras filozofijā. – Rīga: Intelekts, 1997.
37. Kā izveidot EUROPASS CV + EIROPAS PRASMJU PASI [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://www.europass.lv/content/files/EUROPASS_A4_WEB.pdf*
38. Kramiņš E. Retorikas rokasgrāmata. Runāsim skaidri, spilgti, iedarbīgi! – Rīga: SIA "Biznesa augstskola Turība", 2016.
39. Kulturoloģija. 10. klase [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.uzdevumi.lv/p/kulturologija/10-klase*
40. Kulturoloģija. 11. klase [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.uzdevumi.lv/p/kulturologija/11-klase*
41. Kultūras daudzveidība jaunatnes atbalstam, starpkultūru dialoga un daudzvalodības veicināšanai [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.unesco.lv/files/UNESCO_KulturasDaudzveidibaJaunatnesAtbalstam_Papildinats_aeff7564.pdf.*
42. Kūle M. Eirodzīve. – Rīga: FSI, 2006.
43. Lanerī-Dažāna N. Glezniecības enciklopēdija. – Rīga: Jumava, 2006.
44. Language Passport [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680492ff9*
45. Lapiņa M. Latvijas kultūras vēsture 20. gadsimta 40.–80. gados. – Rīga: RaKa, 2002.
46. Lasmane S. 20. gadsimta ētikas pavērsieni. – Rīga: Zvaigzne ABC, 2004.
47. Latvijas jaunā režija. / Projekta vad., zin. red. S. Radzobe. – Rīga: LU Akadēmiskais apgāds, 2015.

48. Latvijas kultūras kanons [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.kulturaskanons.lv*
49. Liotārs Ž. F. Postmodernisma skaidrojums bērniem. // Grāmata. – 1991. – Nr. 12.
50. Latvijas Republikas Kultūras ministrijas tīmekļa vietne [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.km.gov.lv/*
51. Mācību kursa "Starpkultūru komunikācija" rokasgrāmata [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.integration.lv/uploads/files/informativie-materiali/strukturkulturu-komunikacija.pdf*
52. Mitoloģijas enciklopēdija. 1. sēj. – Rīga: Latvijas enciklopēdija, 1993.
53. Mitoloģijas enciklopēdija. 2. sēj. – Rīga: Latvijas enciklopēdija, 1994.
54. Mitoloģijas vārdnīca. / Sast. K. Skruzis. – Rīga: Avots, 2015.
55. Padomes ieteikums (2018. gada 22. maijs) par pamatkompetencēm mūžizglītībā (Dokuments attiecas uz EEZ) (2018/C 189/01) [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32018H0604%2801%29&from=EN*
56. Paiders J. Islams un Rietumi. – Rīga: Zvaigzne ABC, 2001.
57. Pasaules reliģijas. – Rīga: Zvaigzne ABC, 2007.
58. Pitkeviča Inese. Kultūra kā simbolu sistēma [skatīts 2019. gada 22. maijā]. Pieejams: *http://profizgl.lu.lv/pluginfile.php/31818/mod_resource/content/0/Inese_Pitkevica/Prezentacija_simbolu_daudznozimiba_1.pdf*
59. Politiskā komunikācija, ētika un kultūra LR 9. Saeimas vēlēšanās. – Rīga: LU Sociālo un politisko pētījumu institūts, 2007.
60. Priedītis A. Ievads kulturoloģijā. Kultūras teorija un kultūras vēsture. – Daugavpils: A.K.A., 2003.
61. Priedītis A. Kultūru dialogs. – Rīga: Pasaules kultūru fonds, 2006.
62. Projekts "Melu tvertne" [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.diena.lv/melu-tvertne/*
63. Purēns V. Ētika: mācību grāmata. – Rīga: RaKa, 2016.
64. Resnis I. Kas ir latvieši: pašskats. – Rīga: Upe tuviem un tāliem, 2018.
65. Rietumeiropas morāles filozofija. / Sast. S. Lasmane. – Rīga: LU, 2006.
66. Rubenis A. 20. gadsimta kultūra Eiropā. – Rīga: Zvaigzne ABC, 2004.
67. Secretary: job description [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://targetjobs.co.uk/careers-advice/job-descriptions/278955-secretary-job-description*
68. Septiņdesmit pasaules brīnumi. Kā tapa dižākie senatnes pieminekļi. / Red. K. Skerss. – Rīga: Zvaigzne ABC, 2001.
69. Svešvārdu vārdnīca. – Rīga: Norden, 2002.
70. Šlāpins I. Jauno latviešu valoda. – Rīga: Ascendum, 2017.
71. Štukenbroka K., Tepere B. 1000 šedevru Eiropas glezniecībā. 1300–1850. – Rīga: Jāņa Rozes apgāds, 2007.
72. Taivāns L. G., Taivāne E. Reliģiju vēsture. – Rīga: RaKa, 2003.
73. The Implementation of the Common European Framework for Languages in European Education Systems [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/495871/IPOL-CULT_ET(2013)495871(SUM01)_EN.pdf*
74. Tīsenkopfs T. Socioloģija. – Rīga: LU, 2006.
75. TV sižeti par *StartStrong* programmu [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=UYaevWtH5_U&list=PLgIwD9P6S_q45PaOEXvgm6TnPgji51aH3*
76. UNESCO Latvijas dārgumi [skatīts 2019. gada 22. maijā]. Pieejams: *http://latvijasdargumi.unesco.lv/lv/nacionali-noverteti/#map-4*
77. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *http://learnenglishteens.britishcouncil.org/skills/listening*
78. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://agendaweb.org/*

79. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.english-grammar.at/index.htm*
80. Uzdevumu izpilde, izmantojot IT vācu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.hueber.de/shared/uebungen/deutschcom/*
81. Uzdevumu izpilde, izmantojot IT vācu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.deutsch-lernen.com/anfaengerkurs/grammatik_2.php*
82. Uzdevumu izpilde, izmantojot IT vācu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.goethe.de/de/spr/ueb/led.html*
83. Velšs V. Estētikas robeža. – Rīga: Laikmetīgās mākslas centrs, 2005.
84. Vēbers M. Reliģijas socioloģija. – Rīga: LU Filozofijas un socioloģijas institūts, 2004.
85. Vīts Dž. E. Postmodernie laiki. – Rīga: Luterisma mantojuma fonds, 1999.
86. Vudforda S. Kā aplūkot mākslas darbus. – Rīga: Jāņa Rozes apgāds, 2018.
87. Zimmels G. Nauda modernajā kultūrā. // LU Zinātniskie Raksti.– Rīga: LU, 2000. – Nr. 629.
88. Zitāne L. Kultūras vēsture. Kultūras jēdziens un senie laiki. – Rīga: RaKa, 2002.

MODUĻA Valodas, kultūras izpratne un izpausmes (2.līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas apgūt starpkultūru zināšanas un prasmes, veicinot izglītojamo interesi un zinātkāri par valodām un starpkultūru saziņu, pilnveidojot izglītojamo profesionālās saziņas prasmes svešvalodās, kultūras pastāvēšanas un darbības indikatoriem, spēju novērtēt kultūras sasniegumus, vēlmi iesaistīties kultūrprocesu veidošanā, izmantot iegūtās starpkultūru zināšanas profesionālo pienākumu veikšanā un starptautiskās mobilitātes aktivitātēs.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Formulēt savu pasaules izpratni, veidojot pozitīvas attiecības ar dažādu tautību un nacionalitāšu pārstāvjiem. 2. Novērtēt vērtību un ideālu mainības cēloņus dažādās kultūrās. 3. Apzināties savu nacionālo kultūridentitāti, saskatīt savu vietu kultūrprocesu veidošanā. 4. Salīdzināt, analizēt un vērtēt kultūras sasniegumus, liecības un informatīvos avotus. 5. Lietot profesionālajā saziņā vienu svešvalodu un izmantot profesionālo terminoloģiju vismaz divās valodās rakstiski un mutiski.
Moduļa ieejas nosacījumi	Apgūts modulis "Valodas, kultūras izpratne un izpausmes (1. līmenis)".
Moduļa apguves novērtēšana	Moduļa "Valodas, kultūras izpratne un izpausmes (2. līmenis)" apguves noslēgumā izglītojamie kārto pārbaudījumu – prezentē portfolio. Portfolio sadaļas: Intervijas, piemēram, par starpkultūru attiecībām Latvijā. Patstāvīgi izvēlēts teksts par nozares/sektora aktualitātēm (apjoms 5000 rakstu zīmes) un sagatavota prezentācija par izvēlēto tekstu, izmantojot profesionālo terminoloģiju. Argumentētā eseja par kādu no kultūrām, piemēram, "Tradīcijas rietumu un austrumu kultūrā, noturīgais un mainīgais kultūrā". Kāda UNESCO reģistrā iekļauta Latvijas kultūrvēsturiskā objekta prezentācija. Projekta darba rezultātu apkopojums, piemēram, par tādiem kultūras indikatoriem kā nauda vai svētki. EUROPASS CV, motivācijas vēstule (pilnveidoti pēc moduļa "Valodas, kultūras izpratne un izpausmes (1. līmenis)" apguves), aizpildīta anketa, izvērtētas soft skills ("mīkstās prasmes") vienā no svešvalodām. Uzskates līdzekļi – domu kartes, shēmas, tabulas, plāni, kartes, zīmējumi par svešvalodu lietošanu profesionālajā jomā. Gan pedagogs novērtē paveikto 10 ballu skalā, gan izglītojamie savstarpēji novērtē darbus, gan pats izglītojamais savu sasniegumu izvērtē pašnovērtējumā pēc pedagoga sagatavotas pašnovērtējuma veidlapas ar vērtēšanas kritērijiem.
Moduļa nozīme un vieta kartē	Modulis iekļaujams profesionālās izglītības programmās 3. un 4. Latvijas kvalifikāciju ietvarstruktūras līmeņu profesionālās kvalifikācijas apguvei.

MODUĻA Valodas, kultūras izpratne un izpausmes (2.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: formulēt savu pasaules izpratni, veidojot pozitīvas attiecības ar dažādu tautību un nacionalitāšu pārstāvjiem. Zina: jēdzienus integrācija, lojalitāte, starpkultūru attiecības, pozitīva domāšana, uzvedības standarts. Izprot: starpkultūru izglītības lomu integrācijas procesos un līdzdalību sabiedrības dzīvē.	6% no moduļa kopējā apjoma	Izskaidro valodu apguves nozīmību integrācijas procesā. Izskaidro valodas nozīmi pozitīva starpkultūru dialoga veidošanā. Definē jēdzienus integrācija, lojalitāte, starpkultūru attiecības, pozitīva domāšana, uzvedības standarts.	Novērtē valodu apguves nozīmību integrācijas procesā. Pilnveido valodu pozitīva starpkultūru dialoga veidošanai. Minot piemērus, izskaidro jēdzienus integrācija, lojalitāte, starpkultūru attiecības, pozitīva domāšana, uzvedības standarts.
2. Spēj: novērtēt vērtību un ideālu mainības cēloņus dažādās kultūrās. Zina: saistību starp vērtībām, ideāliem un tradīcijām savā un sabiedrības dzīvē. Izprot: kultūras vērtību daudzveidību, raksturojot un novērtējot sabiedrību, pieņemto ideālu, kultūrlaikmeta vērtību sistēmu un normas pasaulē un Latvijā, apzinoties kultūras mantojuma,	12% no moduļa kopējā apjoma	Nosauc vērtību un ideālu mainību cēloņus dažādās kultūrās. Definē jēdzienus kultūras normas, ideāli, nacionālās un internacionālās vērtības, kultūras mantojums, UNESCO, kultūrvaronis, līderis, elks, ģēnijs. Raksturo līdera, kultūrvaroņa, ģēnija, elka vietu un lomu sabiedrībā un kultūrā. Nosauc kultūru savstarpējo saistību pazīmes, iegaumē formu un elementu pārmantojamību pasaules un Latvijas kultūrā. Nosauc UNESCO darbības principus. Nosauc UNESCO reģistrā iekļautos Latvijas kultūrvēsturiskos objektus.	Raksturo un uzskatāmi pierāda vērtību un ideālu mainības cēloņus dažādās kultūrās. Minot piemērus, izskaidro jēdzienus kultūras normas, ideāli, nacionālās un internacionālās vērtības, kultūras mantojums, UNESCO, kultūrvaronis, līderis, elks, ģēnijs. Raksturo un novērtē sabiedrībā pieņemtos ideālus, kultūrlaikmeta vērtību sistēmu un normas pasaulē un Latvijā. Salīdzina un analizē pasaules un Latvijas kultūras informatīvos avotus un liecības. Skaidro UNESCO darbības principus. Nosauc un novērtē savas kultūras izcilākos kultūrobjektus, kas iekļauti UNESCO reģistros.

tradīciju lomu un vērtību pasaules un Latvijas kultūrā.			
3. Spēj: apzināties savu nacionālo kultūridentitāti, saskatīt savu vietu kultūrprocesu veidošanā. Zina: eirocentrisma iezīmes rietumu kultūrā un multikulturālisma pazīmes. Izprot: indivīda un sabiedrības lomu dažādu sabiedrības grupu kultūras veidošanā un pastāvēšanā, saskatot starpkultūru problēmu cēloņus, izvirzot un formulējot starpkultūru komunikācijas iespējas.	12% no moduļa kopējā apjoma	Apraksta masu kultūras un elitārās kultūras pazīmes. Paskaidro atšķirības starp etnisko, nacionālo un multikulturālo identitāti. Sistematizē zināšanas un prasmes par kultūras izpausmju daudzveidību un mijiedarbību mūsdienās. Definē jēdzienu eirocentrisms. Apraksta kādu no pasākumiem un identificē to kā nozīmīgu kultūras pasākumu.	Skaidro un raksturo masu un elitārās kultūras izpausmes formas un liecības. Salīdzina etnisko, nacionālo un multikulturālo identitāti. Klasificē nacionālās un multikulturālās kultūras īpatnības. Pēta un analizē kultūras piederības, konkrētu kultūru pazīmes, kultūras mantojuma, kultūru mijiedarbības un kultūras komercializācijas izpausmes. Raksturo eirocentrisma ideju kā kultūras dialoga konceptu. Argumentēti pamato savu attieksmi eirocentrisma jautājumā. Raksturo un novērtē savu nacionālo kultūridentitāti, saskata savu vietu kultūrprocesu veidošanā.
4. Spēj: salīdzināt, analizēt un vērtēt kultūras sasniegumus, liecības un informatīvos avotus. Zina: indikatoru mijiedarbību dažādās kultūrās. Izprot: kultūras pastāvēšanas un darbības indikatorus un to īpatsvaru kultūras veidošanā.	20% no moduļa kopējā apjoma	Definē jēdzienu kultūras indikatori un nosauc galvenos kultūras indikatorus. Analizē kultūras norišu interpretēšanas robežas. Novērtē savas radošās prasmes.	Atklāj būtiskākos dažādu kultūru indikatorus katrā no kultūrām un min kultūras indikatoru piemērus. Interpretē dažādu indikatoru mijiedarbību dažādās kultūrās, pamato mainīguma iemeslus. Iesaistoties vietēja vai valsts mēroga kultūras notikumos, kā arī radot konkrētai mērķauditorijai paredzētu kultūras produktu, reflektē savas radošās prasmes.
5. Spēj: lietot profesionālajā saziņā vienu svešvalodu un izmantot profesionālo terminoloģiju vismaz divās valodās rakstiski un mutiski. Zina: profesionālo terminoloģiju un valodas apguves iespējas	50% no moduļa kopējā apjoma	Raksturo starpkultūru nozīmi valodas apguvē. Definē valodu prasmes nozīmi karjeras veidošanā, veido Europass CV, motivācijas vēstuli vienā no svešvalodām. Nosauc un analizē informācijas tehnoloģiju izmantošanas iespējas valodu apguvē un darba tirgus izpētē. Lieto profesionālo terminoloģiju.	Ilustrē ar piemēriem un izskaidro starpkultūru nozīmi valodas apguvē. Novērtē valodu prasmes nozīmi karjeras veidošanā. Patstāvīgi veido Europass CV, motivācijas vēstuli, aizpilda anketu. Patstāvīgi izmanto informācijas tehnoloģiju iespējas valodu apguvē un darba tirgus izpētē.

profesionālo zināšanu pilnveidei. Izprot: informācijas tehnoloģiju izmantošanas nozīmīgumu valodu apguvē un darba tirgus izpētē.		Veido vienkāršus tekstus. Aizpilda vai pēc norādījumiem veido ar profesiju saistītu dokumentāciju. Nosauc valodas apguves iespējas profesionālo zināšanu pilnveidei (piemēram, video, lasāmviela, telefonsaruna, dialogs).	Lieto plašu profesionālās leksikas krājumu profesionālajā saziņā. Veido labi strukturētus, detalizētus tekstus. Aizpilda vai patstāvīgi veido ar profesiju saistītu dokumentāciju. Definē priekšrocības un ierobežojumus valodas profesionālās pilnveides avotos. Novērtē savas klausīšanās un runāšanas prasmes līmeņus.

Izmantojamie avoti:

1. Agajevs V. Semiotika. – Rīga: Jumava, 2005.
2. Aldersons J. Mākslas un kultūras vārdnīca ar interneta atslēgvārdiem. – Rīga: Zvaigzne ABC, 2011.
3. Apele A. Prasme runāt publiski. – Rīga: Zvaigzne ABC, 2011.
4. Arnolda D. Saprast mākslu: sešas tēmas. – Rīga: Zvaigzne ABC, 2018.
5. Austruma S., Muižarāja I. Kulturoloģija vidusskolai. – Rīga: Zvaigzne ABC, 2005.
6. Austruma S., Muižarāja I. Kultūras vēsture: metodiskais līdzeklis. – Rīga: ISEC, 2005.
7. Avotiņa A., Blūma D. u.c. Latvijas kultūras vēsture. – Rīga: Zvaigzne ABC, 2003.
8. Avotiņa A., Genese-Plaude I., Mūrnieks A., Pitkeviča I., Voitkāne I. Kulturoloģija kā integrējošs mācību kurss laikmetīgā mācību procesā. – Rīga: LU Pedagoģijas, psiholoģijas un mākslas fakultāte, 2013.
9. Baltijas ceļš [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.thebalticway.eu/*
10. Blūma D. Kultūras vēsture vārdos, jēdzienos un nosaukumos. – Rīga: RaKa, 2000.
11. Bodrijārs Ž. Simulakri un simulācija. – Rīga: Omnia mea, 2000.
12. Ceļā uz darbu [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://www.nva.gov.lv/karjera/docs/_52bcaaf265d237.51951269.pdf*
13. Dempsey A. Modernā māksla. – Rīga: Jāņa Rozes apgāds, 2018.
14. Dubiņa I., Pērkone-Redoviča I. Literatūra un kino. XX gadsimts. Kultūras vēsture. – Rīga: Zvaigzne ABC, 2006.
15. Eiropas kopīgās pamatnostādnes valodas apguvei. Pašnovērtējuma tabula [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://europass.cedefop.europa.eu/sites/default/files/cefr-lv.pdf*
16. Eiropas literatūras vēsture: Hrestomātija. / Annikas Benuā-Dizosuā un Gija Fontēna redakcijā. – Rīga: Jāņa Rozes apgāds, 2013.
17. Eiropas Valodu portfelis (EVP). Principi un vadlīnijas ar paskaidrojumiem [skatīts 2019. gada 7. oktobrī]. Pieejams:
18. *https://valoda.lv/wp-content/uploads/docs/Projekti/LV_mat_evp.pdf*
19. Electrician [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.truity.com/career-profile/electrician*
20. EUROPASS [skatīts 2019. gada 22. maijā]. Pieejams: *http://europass.lv/*
21. Ērgle A., Purēns I., Sviestiņa I. Kulturoloģija. – Rīga: RaKa, 2009.
22. Filma "Latvijas valsts simboli" [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=brB8TrGpkVM*
23. Filma "Pūt, vējiņi. Latvijai 100". Smilšu kino [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=z3RsBKUT6xI*
24. Freids Z. Īgnums kultūrā. – Rīga: Zvaigzne ABC, 2000.

25. Herdera vārdnīca. Simboli. – Rīga: Pētergailis, 199
26. Hodža S., Teilors D. Māksla: enciklopēdija skolēniem. / Tulk. Rute Marta Jansone; red. Ilze Sausiņa. – Rīga: Zvaigzne ABC, 2018.
27. Ierosmes mācību priekšmeta "Kulturoloģija" apguvei. Metodiskais materiāls [skatīts 2019. gada 22. maijā]. Pieejams: *https://visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/kulturologija.pdf*
28. Ilustrētā arhitektūras vēsture. / Emīlijas Kolas redakcijā. – Rīga: Zvaigzne ABC, 2013.
29. Informācijas vide Latvijā: 21. gadsimta sākums. I. Brikšes redakcijā. – Rīga: Zinātne, 2006.
30. Islāms. – Rīga: Zvaigzne ABC, 2004.
31. Jermolajeva J., Jermolajevs V., Mūrnieks A. Kultūras vēsture. 20. gadsimts. – Rīga: RaKa, 2002.
32. Kagaine Z. Tēlainā domāšana vizuālajā mākslā. – Rīga: Zvaigzne ABC, 2005.
33. Kalniņa L., Zvirgzds J. Lielā simbolu enciklopēdija. – Rīga: Jumava, 2006.
34. Karasā F. P., Markadē I. Mākslas enciklopēdija. Glezniecības virzieni. – Rīga: Jumava, 2002.
35. Kasīrers E. Apcerējums par cilvēku. Ievads kultūras filozofijā. – Rīga: Intelekts, 1997.
36. Kā izveidot EUROPASS CV + EIROPAS PRASMJU PASI [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://www.europass.lv/content/files/EUROPASS_A4_WEB.pdf*
37. Kramiņš E. Retorikas rokasgrāmata. Runāsim skaidri, spilgti, iedarbīgi! – Rīga: SIA "Biznesa augstskola Turība", 2016.
38. Kulturoloģija. 10. klase [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.uzdevumi.lv/p/kulturologija/10-klase*
39. Kulturoloģija. 11. klase [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.uzdevumi.lv/p/kulturologija/11-klase*
40. Kultūras daudzveidība jaunatnes atbalstam, starpkultūru dialoga un daudzvalodības veicināšanai [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.unesco.lv/files/UNESCO_KulturasDaudzveidibaJaunatnesAtbalstam_Papildinats_aeff7564.pdf*
41. Kūle M. Eirodzīve. – Rīga: FSI, 2006.
42. Lanerī-Dažāna N. Glezniecības enciklopēdija. – Rīga: Jumava, 2006.
43. Language Passport [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680492ff9*
44. Lapiņa M. Latvijas kultūras vēsture 20. gadsimta 40.–80. gados. – Rīga: RaKa, 2002.
45. Lasmane S. 20. gadsimta ētikas pavērsieni. – Rīga: Zvaigzne ABC, 2004.
46. Latvijas jaunā režija. / Projekta vad., zin. red. S. Radzobe. – Rīga: LU Akadēmiskais apgāds, 2015.
47. Latvijas kultūras kanons [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.kulturaskanons.lv*
48. Liotārs Ž. F. Postmodernisma skaidrojums bērniem. // Grāmata. – 1991. – Nr. 12.
49. Latvijas Republikas Kultūras ministrijas tīmekļa vietne [skatīts 2019. gada 22. maijā]. Pieejams: *http://www.km.gov.lv/*
50. Mācību kursa "Starpkultūru komunikācija" rokasgrāmata [skatīts 2019. gada 22. maijā]. Pieejams: *http://cilvektiesibas.org.lv/site/record/docs/2012/02/07/rokasgramata_starp_kulturu_komunikacija.pdf*
51. Mitoloģijas enciklopēdija. 1. sēj. – Rīga: Latvijas enciklopēdija, 1993.
52. Mitoloģijas enciklopēdija. 2. sēj. – Rīga: Latvijas enciklopēdija, 1994.
53. Mitoloģijas vārdnīca. / Sast. K. Skruzis. – Rīga: Avots, 2015.
54. Padomes ieteikums (2018. gada 22. maijs) par pamatkompetencēm mūžizglītībā (Dokuments attiecas uz EEZ) (2018/C 189/01) [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32018H0604%2801%29&from=EN*
55. Paiders J. Islams un Rietumi. – Rīga: Zvaigzne ABC, 2001.
56. Pasaules reliģijas. – Rīga: Zvaigzne ABC, 2007.

57. Pitkeviča Inese. Kultūra kā simbolu sistēma [skatīts 2019. gada 22. maijā]. Pieejams: *http://profizgl.lu.lv/pluginfile.php/31818/mod_resource/content/0/Inese_Pitkevica/Prezentacija_simbolu_daudznozimiba_1.pdf*
58. Politiskā komunikācija, ētika un kultūra LR 9. Saeimas vēlēšanās. – Rīga: LU Sociālo un politisko pētījumu institūts, 2007.
59. Priedītis A. Ievads kulturoloģijā. Kultūras teorija un kultūras vēsture. – Daugavpils: A.K.A., 2003.
60. Priedītis A. Kultūru dialogs. – Rīga: Pasaules kultūru fonds, 2006.
61. Projekts "Melu tvertne"[skatīts 2019. gada 22. maijā]. Pieejams: *https://www.diena.lv/melu-tvertne/*
62. Purēns V. Ētika: mācību grāmata. – Rīga: RaKa, 2016.
63. Resnis I. Kas ir latvieši: pašskats. – Rīga: Upe tuviem un tāliem, 2018.
64. Rietumeiropas morāles filozofija. / Sast. S. Lasmane. – Rīga: LU, 2006.
65. Rubenis A. 20. gadsimta kultūra Eiropā. – Rīga: Zvaigzne ABC, 2004.
66. Secretary: job description [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://targetjobs.co.uk/careers-advice/job-descriptions/278955-secretary-job-description*
67. Septiņdesmit pasaules brīnumi. / Red. K. Skerss. – Rīga: Zvaigzne ABC.
68. Svešvārdu vārdnīca. – Rīga: Norden, 2002.
69. Šlāpins I. Jauno latviešu valoda. – Rīga: Ascendum, 2017.
70. Štukenbroka K., Tepere B. 1000 šedevru Eiropas gleznieciībā. 1300–1850. – Rīga: Jāņa Rozes apgāds, 2007.
71. Taivāns L. G., Taivāne E. Reliģiju vēsture. – Rīga: RaKa, 2003.
72. The Implementation of the Common European Framework for Languages in European Education Systems [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/495871/IPOL-CULT_ET(2013)495871(SUM01)_EN.pdf*
73. Tīsenkopfs T. Socioloģija. – Rīga: LU, 2006.
74. TV sižeti par *StartStrong* programmu [skatīts 2019. gada 22. maijā]. Pieejams: *https://www.youtube.com/watch?v=UYaevWtH5_U&list=PLgIwD9P6S_q45PaOEXvgm6TnPgji51aH3*
75. UNESCO Latvijas dārgumi [skatīts 2019. gada 22. maijā]. Pieejams: *http://latvijasdargumi.unesco.lv/lv/nacionali-noverteti/#map-4*
76. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *http://learnenglishteens.britishcouncil.org/skills/listening*
77. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://agendaweb.org/*
78. Uzdevumu izpilde, izmantojot IT angļu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.english-grammar.at/index.htm*
79. Uzdevumu izpilde, izmantojot IT vācu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.hueber.de/shared/uebungen/deutschcom/*
80. Uzdevumu izpilde, izmantojot IT vācu valodā [skatīts 2019. gada 10. jūnijā]. Pieejams: *https://www.deutsch-lernen.com/anfaengerkurs/grammatik_2.php*

MODUĻA Iniciatīva un uzņēmējdarbība (1.līmenis) APRAKSTS

Moduļa mērķis	Attīstīt izglītojamo spējas patstāvīgi izstrādāt biznesa ideju, izvērtēt uzņēmējdarbības priekšnosacījumus un biznesa plāna izstrādei nepieciešamo informāciju, veicinot izglītojamo interesi par komercdarbības uzsākšanu, iniciatīvu, radošumu, kritisku domāšanu.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Izskaidrot uzņēmējdarbības pamatjēdzienus. 2. Izstrādāt biznesa ideju. 3. Izvēlēties produktu konkrētai klientu grupai. 4. Noteikt produkta unikālās īpašības. 5. Izmantot svarīgākos produktu izplatīšanas kanālus. 6. Izvēlēties efektīvāko attiecību formātu ar klientu. 7. Prognozēt ienākumu plūsmu. 8. Noteikt nepieciešamos resursus produkta ražošanai. 9. Aprēķināt nodokļus pašnodarbinātām personām. 10. Izvēlēties efektīvākās aktivitātes produkta radīšanai un mārketingam. 11. Izvēlēties atbilstošākos sadarbības partnerus. 12. Aprēķināt izmaksas. 13. Aizpildīt dokumentus, lai reģistrētos par pašnodarbinātu personu. 14. Veikt vienkāršotu grāmatvedības uzskaiti.
Moduļa ieejas nosacījumi	Apgūta pamatizglītība.
Moduļa apguves novērtēšana	Moduļa "Iniciatīva un uzņēmējdarbība (1. līmenis)" apguves gaitā izglītojamie veido portfolio par biznesa ideju, izvēlēto produktu, produkta izplatīšanas kanāliem, naudas plūsmu, nepieciešamajiem resursiem, sadarbības partneriem, piemērojamajiem nodokļiem, dokumentiem, kas nepieciešami, lai reģistrētos par pašnodarbinātu personu, vienkāršotas grāmatvedības uzskaiti un noslēgumā prezentē to.
Moduļa nozīme un vieta kartē	Moduli "Iniciatīva un uzņēmējdarbība (1. līmenis)" īsteno kā mūžizglītības moduli profesionālās pamatizglītības, arodizglītības, profesionālās vidējās un profesionālās tālākizglītības programmās vai neformālās izglītības programmās. Pēc tā apguves var sekot moduļa " Iniciatīva un uzņēmējdarbība (2. līmenis)" apguve.

MODUĻA Iniciatīva un uzņēmējdarbība (1.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: izskaidrot uzņēmējdarbības pamatjēdzienus. Zina: uzņēmējam nepieciešamās rakstura īpašības un kompetences. Izprot: uzņēmēja rakstura īpašību un kompetenču nozīmi uzņēmējdarbībā.	5% no moduļa kopējā apjoma	Nosauc uzņēmējdarbības jēdzienus un raksturo to būtību. Nosauc uzņēmējam nepieciešamās rakstura īpašības un kompetences.	Izskaidro uzņēmējdarbības pamatjēdzienus, raksturo to būtību un nozīmi. Raksturo uzņēmējam nepieciešamās rakstura īpašības un kompetences, ilustrējot to ar vairākiem piemēriem.
2. Spēj: izstrādāt biznesa ideju. Zina: dažādas ideju ģenerēšanas "tehnikas". Izprot: biznesa idejas nozīmi uzņēmējdarbības attīstīšanai.	7% no moduļa kopējā apjoma	Piedalās fragmentāri diskusijā par uzņēmējdarbības sākšanu bez pamatojuma. Piedalās biznesa idejas izstrādē un skaidro to. Uzņēmumam izvēlas nosaukumu.	Pamato savu motivāciju sākt uzņēmējdarbību. Pārliecinoši pamato savu biznesa ideju. Uzņēmumam izvēlas nosaukumu un to pamato.
3. Spēj: izvēlēties produktu konkrētai klientu grupai. Zina: klientu segmentācijas (vispārīgie) pamatprincipi, klientu grupas. Izprot: klienta vajadzības un vēlmes atkarībā no klientu mērķa grupas.	5% no moduļa kopējā apjoma	Nosauc produkta mērķa grupas. Nosauc klientu grupas. Nosauc klientu vajadzības. Vispārīgi raksturo potenciālo klientu. Nosauc labuma saņēmējus no produkta.	Raksturo produkta mērķa grupas. Raksturo klientu grupas. Analizē klientu vajadzības. Detalizēti raksturo potenciālo klientu. Pamato viedokli par labuma saņēmējiem no produkta.
4. Spēj: noteikt produkta unikālās īpašības.	10% no moduļa kopējā apjoma	Nosauc produktu, kuri tiks piedāvāti klientam.	Pamato produkta izvēli, kuri tiks piedāvāti klientam.

Zina: piedāvātā produkta īpašības. Izprot: produkta unikālās vērtības nozīmi klientu izvēlē.		Nosauc taustāmās un netaustāmās produkta īpašības, kuru dēļ klienti pirks produktu. Nosauc klienta ieguvumus, iegādājoties piedāvāto produktu.	Raksturo taustāmās un netaustāmās produkta īpašības, kuru dēļ klienti pirks produktu. Analizē klienta ieguvumus, iegādājoties piedāvāto produktu.
5. Spēj: izmantot efektīvus produkta izplatīšanas kanālus. Zina: produktu izplatīšanas kanālus. Izprot: efektīvu produkta izplatīšanas kanālu izmantošanu klientu piesaistē.	10% no moduļa kopējā apjoma	Nosauc galvenos produkta izplatīšanas kanālus. Izvēlas konkrētus produkta izplatīšanas kanālus.	Raksturo galvenos produkta izplatīšanas kanālus. Pamato izplatīšanas kanālu izvēli.
6. Spēj: izvēlēties efektīvāko attiecību formātu ar klientu. Zina: pirkšanas lēmumu ietekmējošos faktorus. Izprot: klientu rīcību tirgū.	10% no moduļa kopējā apjoma	Nosauc nozīmīgākos saskarsmes pamatprincipus ar klientu. Sasaista pirkšanas lēmumu ar attiecībām ar klientu Nosauc izmaksu pozīcijas attiecību uzturēšanai ar klientiem.	Raksturo nozīmīgākos saskarsmes pamatprincipus ar klientu. Sasaista un izvērtē pirkšanas lēmumu ar attiecībām ar klientu. Analizē izmaksu pozīcijas attiecību uzturēšanai ar klientiem.
7. Spēj: prognozēt ienākumu plūsmu. Zina: ienākumu veidošanās principus. Izprot: regulāru ienākumu nodrošināšanas būtību.	10% no moduļa kopējā apjoma	Nosauc kritērijus, par ko klients gatavs maksāt. Nosauc cenu politikas veidošanas principus. Nosauc maksāšanas veidus. Nosauc ienākumu avotus.	Analizē kritērijus, par ko klients gatavs maksāt. Raksturo cenu politikas veidošanas principus. Analizē maksāšanas veidu priekšrocības un trūkumus. Raksturo ienākumu avotus; analizē ienākumu plūsmu un ienākumu struktūru.
8. Spēj: noteikt nepieciešamos resursus produkta ražošanai. Zina: resursu iedalījumu. Izprot: resursu nozīmi uzņēmējdarbībā.	3% no moduļa kopējā apjoma	Nosauc galvenos resursus un līdzekļus.	Analizē un izvērtē galvenos resursus un līdzekļus.

9. Spēj: aprēķināt nodokļus pašnodarbinātām personām. Zina: nodokļu veidus. Izprot: nodokļu maksāšanas nozīmi.	7% no moduļa kopējā apjoma	Nosauc normatīvos dokumentus nodokļu piemērošanai. Nosauc nodokļu veidus pašnodarbinātām personām. Aprēķina nodokļus pašnodarbinātām personām.	Nosauc normatīvos dokumentus nodokļu piemērošanai. Raksturo nodokļu veidus un nosauc likmes pašnodarbinātām personām. Aprēķina nodokļus pašnodarbinātām personām un analīzē rezultātus.
10. Spēj: izvēlēties efektīvākās aktivitātes produktu radīšanai un mārketingam. Zina: dažādu aktivitāšu ietekmi uzņēmējdarbībā. Izprot: aktivitāšu nozīmi.	10% no moduļa kopējā apjoma	Nosauc galvenās aktivitātes, kas saistītas ar produkta radīšanu, izplatīšanu, klientu piesaisti, ieņēmumiem.	Pamato galvenās aktivitātes, kas saistītas ar produkta radīšanu, izplatīšanu, klientu piesaisti, ieņēmumiem.
11. Spēj: izvēlēties atbilstošākos sadarbības partnerus. Zina: sadarbības partneru darbības specifiku. Izprot: sadarbības partneru izvēles nozīmi.	5% no moduļa kopējā apjoma	Nosauc galvenos sadarbības partnerus. Nosauc galvenos piegādātājus. Nosauc un raksturo iespējamās piegādātāju alternatīvas.	Izskaidro un pamato galveno sadarbības partneru izvēli. Pamato galveno piegādātāju izvēli. Pamato piegādātāju alternatīvu izvēli.
12. Spēj: aprēķināt izmaksas. Zina: izmaksu pozīcijas. Izprot: izmaksu nozīmi uzņēmējdarbībā.	10% no moduļa kopējā apjoma	Nosauc izmaksu veidus un iedalījumu. Nosauc un raksturo būtiskākās izmaksu pozīcijas.	Raksturo izmaksu veidus un iedalījumu. Analizē izmaksu pozīcijas.
13. Spēj: aizpildīt dokumentus, lai reģistrētos par pašnodarbinātu personu. Zina: pašnodarbinātas personas reģistrēšanās procesu.	3% no moduļa kopējā apjoma	Nosauc reģistrēšanās par pašnodarbinātu personu procesa soļus. Aizpilda uzņēmējdarbības reģistrēšanai nepieciešamos dokumentus.	Apraksta reģistrēšanās par pašnodarbinātu personu procesa secīgos soļus. Aizpilda uzņēmējdarbības reģistrēšanai vajadzīgos dokumentus, pamato to nepieciešamību.

Izprot: dokumentu aizpildīšanas nozīmi.			
14. Spēj: veikt vienkāršā ieraksta grāmatvedības uzskaiti. Zina: ieņēmumu un izdevumu pozīcijas. Izprot: grāmatvedības nozīmi uzņēmējdarbībā.	5% no moduļa kopējā apjoma	Skaidro grāmatvedības jēdzienus. Nosauc grāmatvedības mērķus. Nosauc grāmatvedības uzdevumus. Nosauc galvenos grāmatvedības datu izmantotājus. Veic vienkāršotu grāmatvedības uzskaiti.	Izskaidro grāmatvedības un uzskaites jēdzienu atšķirības. Klasificē grāmatvedības īpatnības, uzskaites pamatprincipus. Raksturo grāmatvedības uzdevumus un prasības. Raksturo galvenos grāmatvedības datu izmantotājus un viņu mērķus. Veic vienkāršotu grāmatvedības uzskaiti un analizē rezultātus.

Izmantojamie avoti:

1. Biznesa ABC. Atbalsts uzņēmējiem. [skatīts 2019. gada 3. aprīlī]. Pieejams: *http://www.liaa.gov.lv/lv/biznesa-abc/atbalsts*
2. Biznesa modelēšanā svarīgs ir vērtības piedāvājums [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.luminor.lv/lv/jaunumi-lidz-2017-10-01/eksperts-biznesa-modelesana-svarigs-ir-vertibas-piedavajums*
3. Dubkēvičs L., Ķestere I. Saskarsme. Lietišķā etiķete. Rīga: Jumava, 2003.
4. Eiropas Savenības Padomes ieteikums par pamatkompetencēm mūžizglītībā. 2018 [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32018H0604(01)&from=EN*
5. Iepazīstieties – pavisam citāda prāta vētra! [skatīts 2019. gada 3. aprīlī]. Pieejams: *http://www.kvestnesis.lv/?menu=doc&id=176157*
6. Ievads komunikācijas teorijās [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.alberta-koledza.lv/upload/old/downloads/Ievads_komunik_teorijas.pdf*
7. Ievads uzņēmējdarbībā [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.youtube.com/watch?v=r34hdmOxkAw*
8. Kā atšķiras dažādi digitālās komunikācijas kanāli [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://marisantons.lv/2017/08/14/ka-atskiras-dazadi-digitalas-komunikacijas-kanali/*
9. Kā piesaistīt finansējumu uzņēmējdarbībai [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.seb.lv/info/bizness/ka-piesaistit-finansejumu-uznemejdarbibai*
10. Leibus I. Individuālā uzņēmēja grāmatvedība un nodokļi. – Rīga: Lietišķās informācijas dienests, SIA, 2014.
11. Padomi veiksmīgai attiecību veidošanai un uzturēšanai ar klientu [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.ozols.lv/blog/jaunumi-2/post/padomi-veiksmigu-attiecibu-veidosanai-un-uzturesanai-ar-klientu-33*
12. Pakalpojumi biznesa uzsācējiem [skatīts 2019. gada 3. aprīlī]. Pieejams: *https://www.altum.lv/lv/pakalpojumi/biznesa-uzsacejiem/*
13. Uzņēmējdarbības uzsākšana [skatīts 2019. gada 3. aprīlī]. Pieejams: *http://www.liaa.gov.lv/lv/uznemejdarbibas-uzsaksana*
14. Zaķe Ņ. Uzņēmējdarbība vidusskolām un profesionālās izglītības iestādēm. Rīga: Biznesa augstskola "Turība", 2016
15. The European Entrepreneurship Competence Framework, 2016. [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://publications.jrc.ec.europa.eu/repository/bitstream/JRC101581/lfna27939enn.pdf*

MODUĻA Iniciatīva un uzņēmējdarbība (2.līmenis) APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas patstāvīgi izstrādāt biznesa plānu, izvēloties atbilstošo komercdarbības tiesisko formu un optimālākos finansēšanas avotus, veicinot iniciatīvu, kritisku domāšanu un problēmu risināšanu.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Izvēlēties biznesa idejai piemērotāko komercdarbības formu, finanšu līdzekļu avotus, ievākt nepieciešamo informāciju. 2. Sagatavot naudas plūsmas grafiku, plānot peļņas vai zaudējumu aprēķinu. 3. Veikt tirgus izpēti un datu analīzi, izstrādāt idejas tirgzinības pasākuma plāna īstenošanai. 4. Pieņemt lēmumus par problēmu risinājumu konkrētās situācijās savas profesionālās darbības jomā. 5. Sagatavot prezentāciju un prezentēt biznesa plānu, argumentēt savu viedokli par iegūtajiem rezultātiem. 6. Izveidot un darboties izglītojamo mācību uzņēmumā.[1] [1]pēc izglītojamo izvēles
Moduļa ieejas nosacījumi	Apgūts modulis "Iniciatīva un uzņēmējdarbība (1. līmenis)".
Moduļa apguves novērtēšana	Moduļa "Iniciatīva un uzņēmējdarbība (2. līmenis)" noslēgumā izglītojamais iesniedz un prezentē (individuāli vai grupā) izstrādāto biznesa plānu, ievērojot biznesa plāna struktūru.
Moduļa nozīme un vieta kartē	Moduli "Iniciatīva un uzņēmējdarbība (2. līmenis)" īsteno kā mūžizglītības moduli profesionālās vidējās un profesionālās tālākizglītības programmās vai neformālās izglītības programmās.

MODUĻA Iniciatīva un uzņēmējdarbība (2.līmenis) SATURS

Sasniedzamais mācīšanās rezultāts	Sasniedzamā mācīšanās rezultāta īpatsvars %	Mācību sasniegumu apguves līmeņu apraksti	
		Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: izvēlēties biznesa idejai piemērotāko komercdarbības formu, finanšu līdzekļu avotus, ievākt nepieciešamo informāciju. Zina: komercdarbības tiesiskās formas izvēles kritērijus, uzņēmuma dibināšanas un reģistrēšanas kārtību, finansēšanas formas un avotus, biznesa plāna struktūru. Izprot: biznesa plāna mērķi un nepieciešamību, iekšējās finansēšanas būtību un ārējās finansēšanas piesaistes iespējas un noteikumus.	20% no moduļa kopējā apjoma	Atrod normatīvos aktus, kas regulē uzņēmējdarbību. Nosauc uzņēmējdarbības ierobežojumus. Nosauc uzņēmējdarbības veidus, kuriem nepieciešamas speciālās atļaujas. Nosauc iespējamos saimnieciskās darbības un uzņēmējdarbības veidus. Nosauc uzņēmējdarbības mikrovides un makrovides faktorus. Nosauc konkrētus aktuālās inovācijas piemērus uzņēmējdarbībā Latvijā. Nosauc banku un nebanku finansēšanas veidus un izvēlas savam uzņēmējdarbības veidam atbilstošāko. Sniedz piemērus, raksturojot biznesa plāna izstrādāšanas secību. Nosauc biznesa plāna struktūru un apraksta katrā no biznesa plāna daļām iekļaujamo informāciju. Nosauc uzņēmuma dibināšanai un reģistrēšanai nepieciešamos dokumentus, daļēji tos noformē. Nosauc aktuālās uzņēmējdarbības atbalsta iespējas.	Izskaidro normatīvos aktus, kas regulē uzņēmējdarbību un tās ierobežojumus. Izskaidro galvenās darba devēja un darba ņēmēja tiesības un pienākumus. Izskaidro patērētāju tiesības. Pamato speciālo atļauju (licenču) nepieciešamību. Analizē uzņēmējdarbības ietekmi uz apkārtējo vidi. Raksturo saimnieciskās darbības un uzņēmējdarbības veidus. Raksturo uzņēmējdarbības mikrovides un makrovides faktorus. Izskaidro makrovides faktoru ietekmi konkrētās nozares uzņēmējdarbībā. Raksturo aktuālās inovācijas uzņēmējdarbībā Latvijā un pasaulē un to lietošanas iespējas uzņēmējdarbībā. Min piemērus. Raksturo uzņēmuma finansēšanas veidus. Izvērtē pieejamos banku un nebanku finanšu avotus. Izvēlas un pamato atbilstošāko finansēšanas veidu savas biznesa idejas īstenošanai. Izskaidro biznesa plāna struktūru, identificē ietveramo informāciju. Skaidro katras biznesa plāna daļā iekļaujamās informācijas saturu. Apraksta uzņēmuma dibināšanas un reģistrēšanas procesa soļus. Noformē nepieciešamos uzņēmuma dibināšanas un reģistrēšanas dokumentus. Novērtē aktuālos uzņēmējdarbības finansiālā atbalsta fondus un atbalsta izmantošanas iespējas.

2. Spēj: sagatavot naudas plūsmas grafiku, plānoto peļņas vai zaudējumu aprēķinu bilances izveidei. Zina: finanšu plānošanas procesu un metodes, naudas plūsmas un peļņas/zaudējumu veidošanās pamatprincipus. Izprot: grāmatvedības nozīmi un tai izvirzītās prasības.	35% no moduļa kopējā apjoma	Nosauc grāmatvedības mērķus, uzdevumus, raksturo tās nozīmi uzņēmējdarbībā. Nosauc galvenos grāmatvedības datu izmantotājus. Nosauc uzņēmuma rīcībā esošos saimnieciskos līdzekļus un to veidošanās avotus. Definē saimnieciskās darbības dokumentu Nosauc katra dokumenta galvenos rekvizītus jēdzienus, raksturo tiem izvirzītās prasības. Izskaidro gada pārskata sagatavošanas nepieciešamību. Nosauc gada pārskata sastāvdaļas. Nosauc bilances sastāvu. Sastāda bilanci. Sagatavo plānotās naudas plūsmas pārskatu. Sastāda pelņas vai zaudējumu aprēķinu	Definē grāmatvedības mērķus un uzdevumus. Izskaidro grāmatvedības nozīmi uzņēmējdarbībā. Pamato grāmatvedības uzskaitei izvirzītās prasības. Raksturo galvenos grāmatvedības datu izmantotājus un viņu mērķus. Raksturo uzņēmuma saimniecisko līdzekļu un to veidošanās avotu klasifikāciju. Raksturo saimniecisko līdzekļu grupas. Raksturo grāmatvedības dokumentu klasifikāciju. Noformē vienkāršākos grāmatvedības dokumentus. Izskaidro gada pārskata sastāvdaļu nozīmi un sagatavošanas kārtību. Izskaidro bilances būtību. Sastāda bilanci. Raksturo uzņēmuma finansiālo stāvokli. Sagatavo un izvērtē plānotās naudas plūsmas pārskatu. Sastāda un izvērtē pelņas vai zaudējumu aprēķinu.
3. Spēj: izstrādāt idejas tirgzinības pasākuma plāna īstenošanai., balstoties uz tirgus izpēti un datu analīzi. Zina: tirgus izpētes metodes, tirgzinības pasākuma kompleksa elementus. Izprot: tirgus izpētes nozīmi un tirgzinības pasākumu ietekmi uz biznesa idejas īstenošanu.	20% no moduļa kopējā apjoma	Nosauc tirgzinības iekšējās un ārējās vides faktorus. Nosauc tirgus izpētes metodes, izvēlas atbilstošāko. Veic patērētāju un/vai konkurējošo uzņēmumu izpēti. Apkopo iegūtos tirgus izpētes datus. Nosauc tirgzinības pasākuma kompleksa elementus. Izstrādā tirgzinības pasākumu plānu konkrētam uzņēmumam. Nosauc piemērotākos produkta virzīšanas pasākumu veidus.	Raksturo tirgzinības iekšējās un ārējās vides faktorus. Raksturo tirgus izpētes metodes, novērtē to priekšrocības. Veic patērētāju un/ vai konkurējošo uzņēmumu izpēti. Apkopo un analizē iegūtos tirgus izpētes datus, izskaidro to lietošanas iespējas. Izsaka un pamato savu viedokli par konkrēta uzņēmuma tirgzinības pasākuma kompleksa elementiem. Izstrādā un pamato tirgzinības pasākumu plānu konkrētam uzņēmumam. Izstrādā un analizē piemērotākos produkta virzīšanas pasākumu veidus.
4. Spēj: pieņemt lēmumus par problēmu risinājumu konkrētās situācijās savas profesionālās darbības jomā.	15% no moduļa kopējā apjoma	Nosauc vadīšanas funkcijas un plānu veidus. Apraksta konkrēta uzņēmuma vadības veidu un organizatorisko struktūru. Nosauc darbinieku motivēšanas veidus. Raksturo kontroles nepieciešamību un būtību.	Izskaidro vadīšanas funkcijas būtību un sniedz konkrētus piemērus. Raksturo plāna veidus, pamato to izstrādes nepieciešamību. Izstrādā konkrēta uzņēmuma organizatoriskās un pārvaldes struktūras

Zina: uzņēmuma vadīšanas funkcijas. Izprot: vadīšanas lomu uzņēmējdarbībā.		Nosauc lēmumu pieņemšanas procesa posmus. Balstoties uz konkrēto situāciju, identificē atsevišķus lēmuma pieņemšanas posmus. Paskaidro informācijas un komunikācijas nozīmi lēmumu pieņemšanā.	shēmas, pamato tās. Sasaista uzņēmuma organizatoriskās un pārvaldes struktūru ar darba tiesiskajām normām. Izstrādā darbinieku motivēšanas plānu. Raksturo un izskaidro kontroles nepieciešamību un būtību. Raksturo lēmuma pieņemšanas procesu. Balstoties uz konkrēto situāciju, pieņem lēmumu un to izvērtē. Izskaidro lēmumu pieņemšanas veidus ar piemēriem. Paskaidro un pamato informācijas un komunikācijas nozīmi lēmumu pieņemšanā.
5. Spēj: sagatavot biznesa plānu un argumentēti prezentēt to. Zina: biznesa plāna struktūru, pamatprincipus un kopsakarības. Izprot: biznesa plāna lietojumu praktiskajā darbībā.	10% no moduļa kopējā apjoma	Noformē biznesa plānu, kas iekļauj biznesa plāna pamatelementus. Sagatavo kopsavilkumu, kas vispārīgi dod priekšstatu par izstrādāto biznesa plānu. Vispārīgi izdara secinājumus par iegūtajiem rezultātiem un apraksta priekšlikumus trūkumu novēršanai. Sagatavo vispārīgu prezentāciju, kas kopumā atbilst prasībām. Prezentē savu (savas grupas) biznesa plānu. Nosauc un vispārīgi apraksta iegūtos rezultātus. Kopumā novērtē biznesa idejas dzīvotspēju.	Noformē biznesa plānu, kas pilnībā atbilst biznesa plāna struktūras prasībām. Sagatavo kvalitatīvu biznesa plāna kopsavilkumu, kas dod pilnu un pārliecinošu priekšstatu par izstrādāto biznesa plānu. Apkopo un izdara secinājumus par iegūtajiem aprēķiniem, novērtē tos. Izstrādā kvalitatīvus priekšlikumus uzņēmuma darbības pilnveidošanai, trūkumu novēršanai un efektivitātes paaugstināšanai. Sagatavo prasībām atbilstošu detalizētu prezentāciju. Argumentēti prezentē savu (savas grupas) biznesa plānu, pamato un aizstāv iegūtos rezultātus un analītiski novērtē biznesa idejas dzīvotspēju tirgus apstākļos.

Izmantojamie avoti:

1. Abizāre V. Ievads uzņēmējdarbībā. – Rīga: RaKa, 2004.
2. Alsiņa R., Zolotuhina K., Bojarenko J. Vadības grāmatvedības pamati. – Rīga: RaKa, 2006.
3. Tirgzinību pamati. Autoru kolektīvs. – Rīga: Jumava, 1998.
4. Beļčikovs J., Praude V. Mārketings. – Rīga: Vaidelote, 2006.
5. Biznesa modelis – sniegtie pakalpojumi [skatīts 2019. gada 21. maijā]. Pieejams: *https://www.vases.lv/lv/content/biznesa-modelis-sniegtie-pakalpojumi*
6. Biznesa plāna paraugs jaunam uzņēmumam [skatīts 2019. gada 21. maijā]. Pieejams: *https://www.citadele.lv/common/img/uploaded/doc/loans/biz_plans_jaunam.pdf*
7. Biznesa plāna paraugs. [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.seb.lv/data/pic/SEB-sabiedriba/biznesa_plans_paraugs.doc*

8. Biznesa skice [skatīts 2019. gada 21. maijā]. Pieejams: *https://biznesaskices.lv/*
9. Darba tiesiskās attiecības [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.profesijupasaule.lv/darba-tiesiskas-attieciba*
10. Dokumentu izstrādāšanas un noformēšanas kārtība [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://likumi.lv/ta/id/301436-dokumentu-izstradasanas-un-noformesanas-kartiba*
11. Drukers P. Efektīvs vadītājs. – Rīga: Zoldnera izdevniecība, 2010.
12. Eiropas Savienības Padomes ieteikums par pamatkompetencēm mūžizglītībā. 2018 [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32018H0604(01)&from=EN*
13. Fisks P. Klientu apkalpošanas ģēnijs. – Rīga: Lietišķās informācijas dienests, 2010.
14. Forands I. Biznesa vadības tehnoloģijas. – Rīga: Latvijas Izglītības fonds, 2009.
15. Franšīzes iegūšana – autostrāde uz veiksmi [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.lddk.lv/wp-content/uploads/2014/02/Fransizes_iegusana_autostrade_uz_veiksmi_biznesa.pdf*
16. Grandāne M. u. c. Finanšu grāmatvedība. Mācību līdzeklis. – Rīga: RaKa, 2004.
17. Grigorjeva R., Jesemčika A., Leibus I., Svarinska A. Grāmatvedības pamati. – Rīga: LUMA, 2006.
18. Grigorjeva R., Jesemčika A., Leibus I., Svarinska A. Grāmatvedības pamati uzņēmumos. – Rīga: Lietišķās informācijas dienests, 2014.
19. Hamblina K. Īsi par mārketingu. – Rīga: Jumava, 1995.
20. Jauno uzņēmēju pieredzes stāsti [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.profesijupasaule.lv/jauno-uznemeju-pieredzes-stasti*
21. Ko nozīmē iegādāties franšīzi [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.lvportals.lv/visi/skaidrojumi/245435-ko-nozime-iegadaties-fransizi*
22. Komerclikums [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://likumi.lv/doc.php?id=5490*
23. Labklājības ministrija [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.lm.gov.lv/lv/index.php?option=com_content&view=article&id=80151*
24. Matule I. Grāmatvedības organizācijas dokumenti – izstrādāšanas rokasgrāmata. Rīga: Lietišķās informācijas dienests, 2016.
25. Par grāmatvedību [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://likumi.lv/doc.php?id=66460*
26. Par Latvijas Republikas Uzņēmumu reģistru [skatīts 2019. gada 7. oktobrī]. Pieejams: *https://likumi.lv/doc.php?id=72847*
27. Pelšs A .Vadības grāmatvedība. – Rīga: RTU, 2000.
28. Praude V., Beļčikovs J. Menedžments. Teorija un prakse. Otrais, pārstrādātais izdevums. – Rīga: Vaidelote, 2001.
29. Raņķevica V. Ievads grāmatvedībā. – Rīga: LKA konsultāciju un mācību centrs, 2008.
30. Reklāma un mārketings [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.profesijupasaule.lv/reklama-un-marketings*
31. Ruperte I. Uzņēmuma vadīšana. – Rīga: Jumava, 2010.
32. Saksonova S. Uzņēmējdarbības plānošanas paņēmieni. Mācību līdzeklis. – Rīga: Izglītības soļi, 2004.
33. Sprancmanis N. Uzņēmējdarbības loģistikas pamati. – Rīga: Burtene, 2011.
34. Tirgus zinības [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.liaa.gov.lv/lv/uznemejdarbibas-abc/tirgus-zinibas*
35. Uzņēmējdarbības ABC [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.liaa.gov.lv/lv/uznemejdarbibas-abc/ideja*
36. Uzņēmējdarbības atbalsts [skatīts 2019. gada 21. maijā]. Pieejams: *http://www.profesijupasaule.lv/uznemejdarbibas-atbalsts*
37. Uzņēmumu reģistrs [skatīts 2019. gada 3. jūlijā]. Pieejama: *https://www.ur.gov.lv/*
38. Vai zāle bija zaļāka un debesis zilākas [skatīts 2019. gada 3. jūlijā]. Pieejams: *https://www.csb.gov.lv/lv/sakums*
39. Zaķe Ņ. Uzņēmējdarbība vidusskolām un profesionālās izglītības iestādēm. – Rīga: SIA „Biznesa augstskola Turība", 2016.

40. The European Entrepreneurship Competence Framework. 2016 [skatīts 2019. gada 7. oktobrī]. Pieejams: *http://publications.jrc.ec.europa.eu/repository/bitstream/JRC101581/lfna27939enn.pdf*

Programmas īstenošanai obligāti nepieciešamie materiālie līdzekļi

Nr.p.k.	Materiālie līdzekļi	Daudzums
1.Tehnoloģiskās iekārtas un darba instrumenti		
1.1.	Darba galds un krēsls	1 katram izglītojamajam
1.2.	Aprīkota mācību telpa (tāfele, projektors, dokumentu kamera u.c.)	1 uz grupu
1.3.	Augstas veiktspējas stacionārais vai portatīvais dators, aprīkots ar profesionālām un lietojumprogrammām un pieeju internetam (vēlams arī papildus monitors)	1 katram izglītojamajam
1.4.	Dažādas perifērijas iekārtas	1 uz grupu
1.5.	Multifunkcionālais printeris, kopētājs	1 uz grupu
1.6.	RAID datu glabāšanas ierīce	1 uz grupu
1.7.	Vadu un bezvadu maršrutētājs	1 uz izglītojamo
1.8.	Savienojumu testeri (dažāda tipa tīkla kabeļiem)	1 katram izglītojamajam
1.9.	Dažādi maršrutētāji (Mikrotik, Cisco)	1 uz grupu
1.10.	Tīkla ugunsmūris	1 uz grupu
1.11.	IPS/IDS	1 uz grupu
1.12.	L3 komutatori	1 uz grupu
1.13.	NAS serveris	1 uz grupu
1.14.	Virtualizācijas serveris	1 uz grupu
1.15.	Tīkla drošības testēšanas iekārtas	1uz katru izglītojamo
2.Materiāli, palīgmateriāli u.tml.		
2.1.	Izdrukas papīrs (A4, A3)	Atbilstoši programmas īstenošanai
2.2.	Kancelejas piederumi	Atbilstoši programmas īstenošanai
2.3.	Dažādu veidu LAN kabeļi	Atbilstoši programmas īstenošanai
2.4.	RJ45 konektori	Atbilstoši programmas īstenošanai
2.5.	Knaibles RJ45	1 uz izglītojamo
2.6.	Dažādi tīkla adapteri	1 uz izglītojamo
2.7.	Ārējais HDD/SSD disks	1 uz izglītojamo
2.8	HDD, SSD disku dokstacijas	1 uz izglītojamo
2.9.	Serveru iekārtu rack mount skapis	1 uz grupu
2.10.	USB zibatmiņa	1 uz izglītojamo
2.11.	Dažādas perifērijas iekārtas	1 uz grupu
2.12.	Disku klonēšanas ierīce (Piem., Logicube Falcon Neo)	1 uz grupu
2.13.	Rakstīšanas bloķētājs (Write Blocker)	1 uz grupu
2.14.	SATA un PATA kabelis ar spraudņiem	Atbilstoši programmas īstenošanai
2.15.	Karšu lasītājs (smart-card reader)	1 uz 2
2.16.	Ievainojamību skenēšanas programmatūra (piem. NESSUS)	Atbilstoši programmas īstenošanai
2.17.	Operetājsistēma Windows darba stacijām	1 uz izglītojamo
2.18.	Operetājsistēma Windows server	1 uz grupu
2.19.	Biroja programmatūra MS Office	1 uz izglītojamo
2.20.	Lodāmurs	1 uz izglītojamo

Sagatavotājs: Saldus tehnikums