IZGLĪTĪBAS IESTĀDE	Jelgavas tehnikums
PROGRAMMAS VEIDS	Profesionālās vidējās izglītības programma
PROGRAMMU KOPA	Datorsistēmas, datubāzes un datortīkli
IEGŪSTAMĀ KVALIFIKĀCIJA	**DATORSISTĒMU TEHNIĶIS**, 4.LKI līmenis
IEPRIEKŠĒJĀ IZGLĪTĪBA	Pamatizglītība
ĪSTENOŠANAS ILGUMS	Četri gadi
IEGUVES FORMA	Klātiene

APSTIPRINU tehnikuma
Direktore .....
2024. g „....." . .....

Mācību kursa (moduļa) programma
Datortehnikas drošība

Apjoms stundās: **360 stundas**
Teorija: 120 stundas
Praktiskās mācības: 240 stundas

Stundu sadalījums:

	1. kurss	2. kurss	3. kurss	4.kurss
Teorija		62	58	
Praktiskās mācības		80	160	

Mērķis: Sekmēt izglītojamo spējas uzstādīt datortehniku, veikt apkopi un remontdarbus. Nodrošināt datortehnikas fizisko un loģisko aizsardzību. Veikt datortehnikas un datortīkla inventarizāciju.

Uzdevumi:

Attīstīt izglītojamo prasmes:
1. Piedalīties esošās datortehnikas, programmatūras un esošā datortīkla inventarizācijā.
2. Nodrošināt datortehnikas fizisko drošību.
3. Nodrošināt datortehnikas pievienošanu nepārtrauktai elektrobarošanas padevei.
4. Novērst nesankcionētu programmatūras lietošanu.
5. Nodrošināt datortehnikas pretvīrusu aizsardzību.
6. Informēt lietotājus par datortehnikas pretvīrusu aizsardzību.

Ieejas nosacījumi: Apgūti visi A daļas moduļi.

Apguves novērtēšana: Moduļa apguves noslēgumā izglītojamais kārto moduļa noslēguma pārbaudījumu, kurā ir teorētisko zināšanu pārbaudes jautājumi un praktiskā darba daļa laboratorijā (kabinetā). Izglītojamie:
1. Veic datortehnikas un datortīkla inventarizāciju. Pārbauda datortehniku un tīkla ierīču sarakstu, to tehniskās specifikācijas un konfigurāciju. Novērtē esošo datortehniku un tīkla komponentu stāvokli un sniedz ieteikumus iespējamo labojumu vai jaunu iekārtu ieviešanas nepieciešamībai.
2. Skaidro kādi apstākļi ietekmē datortehnikas un datu drošību. Veic preventīvus pasākumus.
3. Izvērtē un nodrošina datortehnikas fizisko drošību un pievieno to nepārtrauktās elektrobarošanas padevei.
4. Nodrošina datortehnikas pretvīrusu aizsardzību.
5. Izskaidro pretvīrusu aizsardzības nozīmi un aizsardzības pasākumus.

Mācību kursa (moduļa) saturs:

Sasniedzamais rezultāts	Temats	Saturs	Stundu skaits			Mācību sasniegumu apguves līmeņu apraksti	
			Teorija	Praktiskie darbi	Kopā	Vidējs apguves līmenis	Optimāls apguves līmenis
1. Spēj: piedalīties esošās datortehnikas, programmatūras un esošā datortīkla inventarizācijā. Zina: galvenās vienkārša lokālā datortīkla kvalitātes parametrus un uzlabojumu nepieciešamību. Izprot: datorlietotāja vajadzības un	1.1. Datortehnikas, programmatūras un datortīkla inventarizācija. (20% no moduļa kopējā apjoma)	1.1.1. Datortehnikas izvērtēšana.	4	4	**8**	Piedalās datortehnikas atbilstības datorlietotāju prasībām izvērtēšanā.	Izprast datortehnikas tehniskās iespējas un izvērtēt atbilstību datorlietotāju prasībām.
		1.1.2. Datortehnikas ekspluatācijas atbilstība darba prasībām.	4	4	**8**	Novērtē datortehnikas gatavību darbam un ekspluatācijas atbilstību darba aizsardzības prasībām.	Izvērtē un pamato datortehnikas gatavību darbam un ekspluatācijas atbilstību darba aizsardzības prasībām.
		1.1.3. Datortehnikas parametru novērtēšana.	8	8	**16**	Novērtē datortehnikas parametrus un datorlietotāju vajadzības uzlabojumu veikšanai datortīklā (LAN WAN).	Iegūst un izvērtē informāciju datortehnikas uzlabojumu veikšanai datortīklā (LAN WAN) – ātrdarbību, datortehnikas parametriem un datorlietotāju vajadzībām.
		1.1.4. Datortehnikas defekti un kļūmes.	8	4	**12**	Nosaka datortehnikas defektus un datorlietotāju kļūmes darbā ar datortehniku.	Iegūst un izvērtē informāciju datortehnikas uzlabojumu veikšanai, nosaka datortehnikas defektus un datorlietotāju kļūmes darbā ar datortehniku.

datortehnikas veiktspēju.		1.1.5. Lokālā datortīkla kvalitātes parametri.	6	8	**14**	Nosaka galvenos vienkārša lokālā datortīkla kvalitātes parametrus.	Nosaka galvenos vienkārša lokālā datortīkla kvalitātes parametrus un izvērtē uzlabojumu nepieciešamību.
		1.1.6. Uzlabojumi.	4	4	**8**	Novērtē uzlabojumu nepieciešamību.	Izvērtē uzlabojumu nepieciešamību.
2. Spēj: nodrošināt datortehnikas fizisko drošību. Zina: datu aizsardzības pasākumus, kas ir vērsti uz fiziskās piekļuves vadību un ugunsdrošību. Izprot: datortehnikas fiziskās drošības risinājumus un to lietošanu.	2.1. Datortehnikas fiziskā drošība. (15% no moduļa kopējā apjoma)	2.1.1.Datu aizsardzība – fiziskās piekļuves vadība.	4	16	**20**	Izvērtē, identificē, plāno un veic datu aizsardzības pasākumus, kas ir vērsti uz fiziskās piekļuves vadību.	Izvērtē, identificē, plāno, veic un izskaidro datu aizsardzības pasākumus, kas ir vērsti uz fiziskās piekļuves vadību.
		2.1.2. Datu aizsardzība – ugunsdrošība.	6	16	**22**	Izvērtē, identificē, plāno un veic datu aizsardzības pasākumus, kas ir vērsti uz ugunsdrošību.	Izvērtē, identificē, plāno, veic un izskaidro datu aizsardzības pasākumus, kas ir vērsti uz ugunsdrošību.
3. Spēj: nodrošināt datortehnikas	3.1. Datortehnikas pievienošana nepārtrauktai	3.1.1. Elektrobarošanas padeves aprīkojums.	6	4	**10**	Identificē aprīkojumu, kas nodrošina elektrobarošanas padevi.	Identificē un nosauc elektrobarošanas padeves pamatuzdevumus, darbības principus.

pievienošanu nepārtrauktai elektrobarošanas padevei. Zina: datortehnikas pievienošanas nepārtrauktai elektrobarošanas padeves darbībai pamatprincipus un uzbūves īpatnības. Izprot: nepārtraukto elektrobarošanas sistēmu un lietošanu.	barošanas padevei. (10% no moduļa kopējā apjoma)	3.1.2. Elektrobarošanas padeves izvēle.	6	4	**10**	Izvērtē aprīkojumu.	Pamato atbilstošu elektrobarošanas padeves izvēli.
		3.1.3. Aprīkojuma komplektācija.	6	8	**14**	Plāno un veic aprīkojuma komplektāciju.	Novērtē un izskaidro elektrobarošanas padeves pieslēgšanu, kontaktizvadu nozīmi, veic aprīkojuma komplektāciju.
			62	80	**142**		
4. Spēj: novērst nesankcionētu programmatūras lietošanu. Zina: nesankcionētus programmatūras veidus, to izpausmes. Izprot: nesankcionētu programmatūras ietekmi uz iekārtas darbu.	4.1. Nesankcionēta programmatūra (15% no moduļa kopējā apjoma)	4.1.1. Operētājsistēmu un lietojumprogrammatūras aizsardzība.	12	10	**22**	Nodrošina operētājsistēmu un lietojumprogrammatūras aizsardzību pret nesankcionētu/nelicencētu programmatūru.	Nodrošina un identificē operētājsistēmu un lietojumprogrammatūras aizsardzību pret nesankcionētu/ nelicencētu programmatūru, raksturo tās ietekmi uz iekārtu darbu.
		4.1.2. Datortehnikas un lokālo datortīklu aizsardzība.	14	16	**30**	Nodrošina datortehnikas vienību un lokālo datortīklu fizisko aizsardzību.	Nodrošina un izskaidro datortehnikas vienību un lokālo datortīklu fizisko aizsardzību veidu nozīmi,

							analizē, piedāvā labākos risinājumus.
5. Spēj: nodrošināt datortehnikas pretvīrusu aizsardzību. Zina: pretvīrusu programmatūras, to darbības veidus. Izprot: vīrusa programmas ietekmi uz iekārtu un tīkla darbību.	5.1. Datortehnikas pretvīrusu aizsardzība. (15% no moduļa kopējā apjoma)	5.1.1. Datu aizsardzības pasākumu identificēšana.	2	4	**6**	Identificē datu aizsardzības pasākumus.	Identificē un izvērtē datu aizsardzības pasākumus.
		5.1.2. Datu aizsardzības plānošana.	4	8	**12**	Veic datu aizsardzības pasākumus.	Plāno un veic datu aizsardzības un lietotāja kontu aizsardzības pasākumus.
		5.1.3. Ugunsmūris.	4	6	**10**	Lieto ugunsmūri.	Raksturo ugunsmūru veidus. Izskaidro to darbības principus un lietojumu.
		5.1.4. Pretvīrusu programmatūra.	4	8	**12**	Lieto pretvīrusu programmatūru.	Uzstāda un lieto pretvīrusu programmatūru, izvērtē un sniedz labāko risinājumu.
		5.1.5. Diagnostikas programmatūra.	4	8	**12**	Lieto diagnostikas programmatūru	Jēgpilni pielietojot diagnostikas programmatūru nosaka problēmcēloņus.
6. Spēj: informēt lietotājus par datortehnikas pretvīrusu aizsardzību. Zina: datorsistēmu loģiskās aizsardzības rīkus. Izprot: pretvīrusu aizsardzības pasākumu nozīmīgumu.	6.1. Darbs ar lietotāju. (25% no moduļa kopējā apjoma)	6.1.1. Ugunsmūra lietošana.	20	20	**40**	Informē lietotājus par ugunsmūra lietošanu.	Lieto un konfigurē ugunsmūri pretvīrusu aizsardzībai.
		6.1.2. Pretvīrusu programmatūru lietošana.	20	28	**48**	Informē lietotājus par pretvīrusu programmatūras lietošanu.	Analizē pretvīrusu programmatūras piedāvājumu. Salīdzina antivīrusu programmas un izvēlās piemērotāko. Instalē pretvīrusu programmatūru un veic tās uzturēšanu.
Noslēguma pārbaudījums: ieskaite			**2**	**4**	**6**		
Kopā:			**120**	**240**	**360**		

Mācību kursa īstenošanai izmantojamās mācību metodes: Avotu analīze, diskusija, tests, praktiskais darbs, pētnieciskais darbs, situāciju modelēšana, mācību ekskursija, prezentācija, izpēte.

Izmantotie avoti:

1. Esi drošs [skatīts: 20.09.2024.]. Pieejams: https://www.esidross.lv/
2. Informācijas drošība un privātums datorzinātnē [skatīts: 20.09.2024.]. Pieejams: https://enciklopedija.lv/skirklis/4467-inform%C4%81cijas-dro%C5%A1%C4%ABba-un-priv%C4%81tums,-datorzin%C4%81tn%C4%93
3. Informācijas un komunikācijas tehnoloģiju pamatjēdzieni [skatīts: 20.09.2024.]. Pieejams: https://profizgl.lu.lv/mod/book/view.php?id=22319
4. Kiberincidentu novēršanas institūcija [skatīts: 20.09.2024.]. Pieejams: https://www.cert.lv/lv/
5. Ugunsmūris [skatīts: 20.09.2024.]. Pieejams: https://computer.howstuffworks.com/firewall.htm

Programmu izstrādāja:_____ Daiga Dumpe

SASKAŅOTS

Metodiskās komisijas priekšsēdētāja

..... Judīte Poriķe

2024.g. „.....” septembrī.

Protokola Nr.....