Eiropas Sociālā fonda projekts "Nozaru kvalifikācijas sistēmas izveide un profesionālās izglītības efektivitātes un kvalitātes paaugstināšana" (vienošanās Nr.2010/0274/1DP/1.2.1.1.1/10/IPIA/VIAA/001)

MODUĻA "EIKT drošības politikas veidošana" APRAKSTS

Moduļa mērķis	Sekmēt izglītojamo spējas līdzdarboties uzņēmuma EIKT drošības politikas veidošanā un datu aizsardzības nodrošināšanā.
Moduļa uzdevumi	Attīstīt izglītojamo prasmes: 1. Organizēt drošu datu glabāšanas un apmaiņas kārtību. 2. Iepazīstināt datorlietotāju ar drošu informācijas glabāšanu, ļaundabīgo programmatūru, tās veidiem un izpausmēm un datorsistēmu un lokālo datortīklu fizisko aizsardzību, datu rezerves kopiju veidošanu.
Moduļa ieejas nosacījumi	Datorsistēmu tehniķa profesijas izglītojamie ir apguvuši moduļus "Biroja tehnikas apkope un remonts" un "Serveru izvēle un uzstādīšana". Programmēšanas tehniķa profesijas izglītojamie apguvuši moduli "Serveru izvēle un uzstādīšana". Telekomunikāciju tehniķa izglītojamie ir apguvuši moduļus "Lokālo tīklu ierīkošana" un "Biroja tehnikas apkope un remonts".
Moduļa apguves novērtēšana	Moduļa apguves noslēgumā izglītojamie kārto ieskaiti, kurā ietverta teorētisko zināšanu pārbaude un praktiskie darbi. Ieskaites teorētiskajā daļā tests zināšanu kontrolei, praktiskajā daļā – projekta darbs (izglītojamie izveido drošības politiku savam uzņēmumam, izvēloties rīkus fiziskajai un loģiskajai drošībai.).
Moduļa nozīme un vieta kartē	Modulis "EIKT drošības politikas veidošana" ir B daļas modulis. Programmēšanas tehniķa profesijas izglītojamie moduli "EIKT drošības politikas veidošana" apgūst vienlaicīgi ar moduli "Datu bāzu programmēšana", Telekomunikāciju tehniķa profesijas izglītojamie apgūst moduli vienlaicīgi ar "Ārējo vadu un bezvadu telekomunikāciju tīklu ierīkošana un uzturēšana". Pēc moduļa "EIKT drošības politikas veidošana" seko prakses moduļi.

MODUĻA "EIKT drošības politikas veidošana" SATURS

Sasniedzamais rezultāts	Temats	Ieteicamais saturs	Mācību sasniegumu apguves līmeņu apraksti		Metodiskais nodrošinājums	
			Vidējs apguves līmenis	Optimāls apguves līmenis	Metodiskie paņēmieni un mācību organizācijas formas	Idejas īstenošanai
1. Spēj: organizēt datu glabāšanas un apmaiņas kārtību. Zina: datu glabāšanas un apmaiņas, datu aizsardzības organizēšanas kārtību. Izprot: drošas informācijas glabāšanas nozīmi datorlietotāja darbā.	1.1. Datu glabāšana un informācijas apmaiņa. (25% no moduļa kopējā apjoma)	1.1.1. Datu glabāšanas ierīce.	Raksturo datu glabāšanas ierīču veidus, atšķir datu glabāšanas ierīču lietojumu.	Izvērtē un izvēlas datu glabāšanas uzdevumam atbilstošāko datu glabāšanas ierīci.	Prāta vētra.	Prāta vētrā izglītojamie nosauc datu glabāšanas ierīces, grupējot tās pēc: ierakstīšanas, glabāšanas, piekļuves un izvietojuma (fiziskās atrašanās) veidiem.
					Krustvārdu mīkla.	Izglītojamie veido krustvārdu mīklu no datu glabāšanas ierīču nosaukumiem, apmaiņās un aizpilda to.
					Prezentācija.	Izglītojamie pāros veido prezentācijas par datu glabāšanas ierīcēm, to raksturlielumiem, darbības principiem, priekšrocībām un trūkumiem.
					Diskusija.	Diskusijā izglītojamie pieņem lēmumu, kāda datu glabāšanas ierīce ir vispiemērotākā datu glabāšanai konkrētā gadījumā.
					Patstāvīgais	Laboratorijas darbā

					darbs.	izglītojamie veic datu saglabāšanu vairākās datu glabāšanas ierīcēs, veicot mērījumus pēc raksturotājlielumiem: kapacitāte, piekļuves ātrums, izturība, iespēja piekļūt datiem no dažādām ierīcēm, datu glabāšanas izmaksas uz vienu datu vienību.
		1.1.2. Datu aizsardzības organizēšanas kārtība.	Organizē datu aizsardzības kārtību.	Izskaidro datu aizsardzības procesu, piedāvā risinājumus datu aizsardzības procesa optimizācijai	Mācību ekskursija.	Izglītojamie klātienē tiekas ar IT speciālistiem, kuri organizē datu aizsardzību uzņēmumā, pēc ekskursijas aizpilda darba lapas ar jautājumiem par datu aizsardzības organizēšanu. Izglītojamie iepazīstas ar uzņēmuma drošības politiku, ierakstot informāciju sagatavotā tabulā par datu aizsardzības pasākumiem.
					Argumentēta eseja.	Izglītojamie raksta argumentētu eseju par datu aizsardzības organizēšanas kārtību.
		1.1.3. Datu kopiju veidošana.	Veido, pārbauda un atjauno datu kopijas, izmantojot instrukcijas.	Novērtē datu nozīmīgumu un pieņem lēmumu par datu kopiju veidošanas nosacījumiem (izvēlas datu	Izpēte.	Izglītojamie veic pētījumu par datu rezerves kopiju veidošanas nepieciešamību (biežumu, datu apjomu) un nosacījumiem tās veikšanai.
					Diskusija.	Diskusijā izglītojamie noskaidro, kādiem datiem

				glabāšanas ierīci, datu apjomu, kopiju veidošanas biežumu), pārbauda un atjauno datus.		nepieciešams veikt biežāku rezerves kopiju izveidi, kādi nosacījumi jāievēro rezerves kopiju glabāšanai.
					Patstāvīgais darbs.	Laboratorijas darbā izglītojamie izvēlas datu glabāšanas ierīci un veic datu rezerves kopēšanu, pamatojot savu izvēli.
		1.1.4. Datu apmaiņa.	Veic drošu datu apmaiņu.	Analizē nepieciešamo datu apmaiņas procesu, piedāvā drošākos risinājumus datu apmaiņai.	Informācijas tehnoloģiju izmantošana.	Izglītojamie internetā meklē informāciju par drošas datu apmaiņas veidiem, veido aprakstu par datu apmaiņas protokoliem, datu šifrēšanu, e-paraksta lietošanu.
					Izpēte.	Mācību pētījums "Datu apmaiņas iespējas", kurā izglītojamie pēta datu apmaiņas veidus: ārējās datu glabāšanas ierīces, datu apmaiņa internetā, datu koplietošana, mākoņskaitļošanas tehnoloģijas. Salīdzina datu apmaiņas veidu priekšrocības un trūkumus, drošību, resursu patēriņu, prasības lietotājiem un tehnikai.
2. Spēj: iepazīstināt datorlietotāju ar drošu informācijas glabāšanu. Zina: datu glabāšanas	2.1. Datu aizsardzība un droša informācijas glabāšana. (20% no moduļa	2.1.1. Personas datu aizsardzība (dati, procesi, datu subjekts, personas dati, sensitīvie dati, datu apstrādes sistēmas).	Apraksta vispārīgi personas datu aizsardzības nepieciešamību. Iepazīstina lietotājus ar drošas	Argumentē personas datu aizsardzības nepieciešamību. Raksturo datu apstrādes sistēmas izveidošanas un	Darbs ar tekstu.	Izglītojamie iepazīstas ar fizisko personu datu aizsardzības likumu, atbildot uz jautājumiem par terminiem, datu subjekta tiesībām, sensitīviem

un apmaiņas kārtību, datu aizsardzību un iznīcināšanu no neizmantojamiem vai bojātiem datu nesējiem. Izprot: drošas informācijas glabāšanas nozīmi datorlietotāja darbā un personas datu aizsardzībā.	kopējā apjoma)		informācijas glabāšanas principiem.	uzturēšanas noteikumus, izskaidro datorlietotājiem personas datu aizsardzības prasības.		datiem, sistēmas veidošanas un uzturēšanas nosacījumiem.
					Diskusija.	Izglītojamie diskutē, kādām iestādēm un uzņēmumiem nepieciešams reģistrēt datu apstrādes sistēmas, pārrunā gadījumus, kad paši izglītojamie kā datu subjekti ir piekrituši personīgo datu apstrādei.
		2.1.2. Privāto datu apdraudējumi un aizsardzība.	Lieto aizsardzības līdzekļus privāto datu drošībai.	Argumentē datu aizsardzības līdzekļu izvēli un izskaidro drošības pasākumu nozīmi.	Praktiskais darbs.	Izglītojamie noskaidro privāto datu apdraudējumus globālajā tīmeklī, noskaidro datu aizsardzības līdzekļus, veic privāto datu aizsardzību ar kādu no metodēm.
		2.1.3. Datu atgūšana no bojātiem datu nesējiem. Datu iznīcināšana.	Veic drošu datu iznīcināšanu pēc instrukcijas. Atgūst datus no bojātām datu glabāšanas ierīcēm. Prezentē lietotājiem prezentāciju par datu drošību un aizsardzību.	Piemēro pareizu datu iznīcināšanas veidu. Raksturo datu atgūšanas iespējas, izvēlas optimālāko datu atgūšanas veidu un atgūst datus no bojātām datu glabāšanas ierīcēm, raksturo datu drošību un aizsardzību lietotājiem. Analizē lietotāju situāciju datu drošībā un piedāvā piemērotāko risinājumu datu	Informācijas tehnoloģiju izmantošana.	Izglītojamie izpēta internetā piedāvātos datu atgūšanas rīkus, apraksta nosacījumus, kas ietekmē datu atgūšanas iespējamību, apraksta datu tipiem atbilstošākos datu atgūšanas rīkus.
					Praktiskais darbs.	Praktiskajā darbā izglītojamie atgūst datus no bojāta cietā diska, formatētas atmiņas kartes.
					Laboratorijas darbs.	Datu iznīcināšana – izglītojamie dzēš datus no datu nesēja ar dažādām metodēm, tos pašu datus atgūst, salīdzinot, kāds datu apjoms ir atgūstams, lietojot

				aizsardzībai.		dažādas datu iznīcināšanas metodes.
					Prezentācija.	Izglītojamie veido prezentāciju datorlietotāju vajadzībām: "Kādi faktori ietekmē datu drošību, kā aizsargāt savus personīgos datus, uzņēmuma datus no ļaunprātīgiem uzbrukumiem?" Izglītojamie veic prezentāciju vērtējumu.
3. Spēj: iepazīstināt datorlietotāju ar ļaundabīgo programmatūru, tās veidiem un izpausmēm. Zina: ļaundabīgo programmatūru. veidus, to izpausmes. Izprot: ļaundabīgās programmatūras ietekmi uz iekārtas darbu.	3.1. Ļaundabīgā programmatūra. (20% no moduļa kopējā apjoma)	3.1.1. Ļaundabīgās programmatūras veidi (vīrusi, tārpi, Trojas zirgi, spiegošanas programmas, reklāmprogrammatūra).	Nosauc ļaundabīgās programmatūras veidus, kaitējumu, ko programmatūra var nodarīt datiem un ierīcēm.	Identificē ļaundabīgās programmatūras veidus, raksturo tās ietekmi uz iekārtu darbu.	Referāts.	Izglītojamie raksta referātu, aprakstot ļaundabīgās programmatūras veidus.
					Prezentācija.	Izmantojot internetu, izglītojamie grupās (3-4 grupā) veido prezentāciju par jaunākajām kaitniecības programmām.
					Spēle.	Izglītojamie "burtu režģī" meklē ļaundabīgo programmu nosaukumus un apraksta tos.
		3.1.2. Datortīklu apdraudējumi (tīkla pakešu analizatori, IP-adrešu atdarināšana, uzbrukumi ar parolēm, iekšējās informācijas pārraide objektiem ārpus tīkla, uzbrukumi no tīkla iekšpuses).	Nosauc datortīklu apdraudējumus.	Identificē datortīklu apdraudējumus, raksturo apdraudējumu izpausmes un sekas.	Eseja.	Izglītojamie raksta argumentētu eseju "Datortīkla drošības apdraudējumi". Izglītojamie no interneta apkopo datus par biežākajiem datortīkla apdraudējumiem un apdraudējumu veidiem, iespējamajiem risinājumiem, ietverot informāciju esejā.

		3.1.3. Darbs ar lietotāju.	Iepazīstina datorlietotāju ar ļaundabīgo programmatūru, tās veidiem un izpausmēm, apraksta ļaundabīgās programmatūras ietekmi uz datu drošību un ierīču darbu. Lieto veiksmīgas saskarsmes pamatprincipus.	Izskaidro lietotājam ļaundabīgās programmatūras ietekmi uz datu drošību un ierīču darbu. Veido patīkamu saskarsmi ar dažāda tipa cilvēkiem.	Praktiskais darbs.	Izglītojamie veido prezentāciju par ļaundabīgo programmatūru, tās izpausmes veidiem un ietekmi uz iekārtu darbu.
					Diskusija.	Izglītojamie grupās diskutē par komunikāciju prasmēm, faktoriem, kas ietekmē veiksmīgas sarunas veidošanos. Prezentē savu darbu citām grupām.
4. Spēj: iepazīstināt datorlietotāju ar datorsistēmu un lokālo datortīklu aizsardzību. Zina: datu aizsardzības nosacījumus, fiziskās vides faktoru ietekmi uz datortehnikas iekārtām un sekas. Izprot: datorsistēmu un lokālo tīklu aizsardzības nozīmi to drošai un ilgtspējīgai darbībai.	4.1. Datorsistēmu un tīklu fiziskā aizsardzība. (15% no moduļa kopējā apjoma)	4.1.1. Fiziskās aizsardzības veidi (programnodrošinājums, ierobežota piekļuve, komunikāciju plāns, elektroenerģijas nodrošinājums).	Raksturo datorsistēmas un tīklu fiziskās aizsardzības veidu nozīmi, fiziskās aizsardzības pasākumu kopumu.	Izskaidro datorsistēmas un tīklu fiziskās aizsardzības veidu nozīmi, analizē datorsistēmas un tīklu fizisko aizsardzību, piedāvā risinājumus fiziskās drošības uzlabošanai.	Tests.	Izglītojamie izstrādā testu ar jautājumiem par faktoriem, kas jāievēro, veidojot fizisko datu aizsardzību, savstarpēji apmainās ar tiem un aizpilda.
					Patstāvīgais darbs.	Izglītojamie individuāli izpēta un piedāvā elektroenerģijas nodrošinājuma risinājumus.
					Situācijas modelēšana.	Izglītojamie grupās (3-4 grupā) pēc iepriekš dota apraksta veido fiziskās aizsardzības modeli, prezentē to pārējām grupām, diskutē par risinājumu piemērotību.
		4.1.2. Serveru fiziska aizsardzība (nesankcionēta piekļuve, neatbilstoši klimatiskie	Atpazīst faktorus, kas apdraud datu drošību serveros. Nodrošina datu	Raksturo datu drošības apdraudējuma faktorus serverī.	Patstāvīgais darbs.	Izglītojamie aizpilda patstāvīgā darba lapas par serveru telpas ierīkošanas tehniskajiem nosacījumiem.

		apstākļi, ugunsgrēks, plūdi, elektroenerģijas padeves pārtraukumi, tīši bojājumi).	drošību serveros.	Piemēro profilakses faktoru riska novēršanai, piedāvā risinājumus drošai datu glabāšanai serverī.	Diskusija.	Izglītojamie diskutē par serveru telpas tehnisko nosacījumu ietekmi uz datu drošību.
					Grupu darbs.	Izglītojamie grupās (3-4 grupā) sagatavo priekšlikumu serveru telpas aprīkojumam pēc darba uzdevumā norādītajiem kritērijiem.
	4.2. Datorsistēmas un tīklu loģiskā aizsardzība. (20% no moduļa kopējā apjoma)	4.2.1. Loģiskās aizsardzības veidi (lietotāju tiesības, grupu politika, paroles, lietotāju autorizācija, datu šifrēšana, sistēmas žurnālu lietojums, pārraudzības (monitoringa) izveide).	Veido datorsistēmas un tīklu loģiskās aizsardzības pasākumu kopumu.	Izskaidro datorsistēmas un tīklu loģiskās aizsardzības veidu nozīmi, analizē datorsistēmas un tīklu fizisko aizsardzību, piedāvā risinājumus loģiskās drošības uzlabošanai.	Problēmas risinājums.	Pēc situācijas apraksta izglītojamie veido diagrammu par grupu politikas veidošanai, lietotāju tiesību piešķiršanu.
					Patstāvīgais darbs.	Laboratorijas darbā izglītojamie dala lietotājus grupās, nosaka tiesības, pievieno autorizācijas noteikumus.
					Diskusija.	Izglītojamie diskutē par drošām parolēm un to veidošanas un glabāšanas nosacījumiem.
					Patstāvīgais darbs.	Izglītojamie veido aprakstu par šifrēšanas veidiem un salīdzina to priekšrocības un trūkumus.
					Grupu darbs.	Izglītojamie grupās (3-4 grupā) risina problēmu par datu plūsmas kontroli uzņēmumā, plāno savu darbu, apkopo rezultātus, tos prezentē un izvērtē rezultātu.

		4.2.2. Ugunsmūris (programmatūras, aparatūras maršrutētājs, bezvadu maršrutētājs).	Nosauc ugunsmūru veidus. Izskaidro aparatūras ugunsmūra nozīmi un iespējas datu drošības uzlabošanai.	Raksturo ugunsmūru veidus. Izskaidro to darbības principus un lietojumu.	Patstāvīgais darbs.	Individuālajās darba lapās aizpilda tabulu par ugunsmūru funkcijām. Laboratorijā izglītojamie uzstāda ugunsmūrus, tos konfigurē atbilstoši darba aprakstam. Testē ugunsmūru drošību.
		4.2.3. Pretvīrusu programmatūra.	Vispārīgi raksturo pretvīrusu programmatūru. Izskaidro uzstādīšanas prasības un atjauninājumu nepieciešamību. Instalē pretvīrusu programmatūru.	Analizē pretvīrusu programmatūras piedāvājumu. Salīdzina antivīrusu programmas un izvēlās piemērotāko. Instalē pretvīrusu programmatūru un veic tās uzturēšanu.	Patstāvīgais darbs.	Izglītojamie apkopo pretvīrusu programmu piedāvājumu no interneta, izvēloties 3 piemērotākās, pamato savu izvēli. Laboratorijā izglītojamie instalē un konfigurē izvēlēto pretvīrusu programmatūru.

Ieteicamie avoti

Datu aizsardzība [skatīts 2015. gada 21. aprīlī]. Pieejams: *https://www.esidross.lv/*
Datu drošība [skatīts 2014. gada 8. decembrī]. Pieejams: *https://www.cert.lv/*
Drošība tiešsaistē [skatīts 2015. gada 21. aprīlī]. Pieejams: *https://ssd.eff.org/en/*
Drošības pasākumi tiešsaistē [skatīts 2015. gada 21. aprīlī]. Pieejams: *http://makeitsecure.org/en/index.html*
Fizisko personu datu aizsardzības likums [skatīts 2014. gada 8. decembrī]. Pieejams: *http://likumi.lv/doc.php?id=4042/*
Informācijas tehnoloģiju drošības likums [skatīts 2014. gada 8. decembrī]. Pieejams: *http://likumi.lv/doc.php?id=220962/*
Lietotāju grupu veidošana Windows vidē [skatīts 2015. gada 21. aprīlī]. Pieejams: *http://windows.microsoft.com/lv-lv/windows/user-groups#1TC=windows-7/*
Ministru kabineta 2001. gada 30. janvāra noteikumi Nr. 40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" [skatīts 2014. gada 8. decembrī]. Pieejams: *http://likumi.lv/doc.php?id=2697/*
Pretvīrus programmatūra [skatīts 2015. gada 21. aprīlī]. Pieejams: *http://www.pcantivirusreviews.com/Comparison/*
Ugunsmūris [skatīts 2015. gada 21. aprīlī]. Pieejams: *http://computer.howstuffworks.com/firewall.htm*
Vēzis V. Datortīkli un interneta pakalpojumu izmantošana. – Rīga: Mācību grāmata, 2000.

MODUĻA "EIKT drošības politikas veidošana" ĪSTENOŠANAI NEPIECIEŠAMIE MATERIĀLIE LĪDZEKĻI

Nr.p.k.	Materiālie līdzekļi	Daudzums
1.	**Tehnoloģiskās iekārtas un darba instrumenti**	
1.1.	Stacionārais dators, aprīkots ar profesionālām un lietojumprogrammām un pieeju internetam	1 katram izglītojamajam
1.2.	Cietais disks	1 uz 4 izglītojamajiem
1.3.	Cietvielu disks	1 uz 4 izglītojamajiem
1.4.	Optiskais disks	1 katram izglītojamajam
1.5.	Diski (matricas) vai zibatmiņa	1 katram izglītojamajam
1.6.	RAID datu glabāšanas ierīce	1 uz grupu
1.7.	Maršrutētājs	1 uz 2 izglītojamajiem
1.8.	Bezvadu maršrutētājs	1 uz 2 izglītojamajiem
2.	**Materiāli, palīgmateriāli u.tml.**	
-	-	-