| | |
|---|---|
| IZGLĪTĪBAS IESTĀDE | Rēzeknes tehnikums |
| PROGRAMMAS VEIDS | Profesionālā vidējā izglītība |
| PROGRAMMAS NOSAUKUMS | Programmēšana, 33 484 011 |
| IEGŪSTAMĀ KVALIFIKĀCIJA | Programmēšanas tehniķis, trešais profesionālās kvalifikācijas līmenis |
| IEPRIEKŠĒJĀ IZGLĪTĪBA | Pamatizglītība |
| ĪSTENOŠANAS ILGUMS | Četri gadi ( 5768 stundas ) |
| ĪSTENOŠANAS FORMA | Klātiene |

**APSTIPRINU:**

Rēzeknes tehnikuma

direktore _____ B. Virbule

2019. gada 2. septembrī

Moduļa programma

# EIKT drošības politikas veidošana

**Apjoms stundās: 248 stundas**

| | |
|---|---|
| Teorija | 140 stundas |
| Prakse | 108 stundas |

**Stundu sadalījums semestros:**

| Stundu veids | 1. semestris | 2. semestris | 3. semestris | 4. semestris | 5. semestris | 6. semestris | 7. semestris | 8. semestris |
|---|---|---|---|---|---|---|---|---|
| Teorija | | | | | | 48 | 92 | |
| Prakse | | | | | | 30 | 78 | |
| Patstāvīgais darbs | | | | | | | | |
| Kopā | | | | | | **78** | **170** | |

**Mērķis:** Sekmēt izglītojamo spējas līdzdarboties uzņēmuma EIKT drošības politikas veidošanā un datu aizsardzības nodrošināšanā.

**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".

**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.).

| Sasniedzamais rezultāts | Temats | Ieteicamais saturs | Mācību sasniegumu apguves līmeņu apraksti | | Stundu skaits | | | **Obligātā pārbaudes darba veids** |
|---|---|---|---|---|---|---|---|---|
| | | | Vidējs apguves līmenis | Optimāls apguves līmenis | Teorija | Prakse | Kopā | |
| **6. semestris** | | | | | | | | |
| 1. Spēj: organizēt datu glabāšanas un apmaiņas kārtību.<br><br>Zina: datu glabāšanas un apmaiņas, datu aizsardzības organizēšanas kārtību.<br><br>Izprot: drošas informācijas glabāšanas nozīmi datorlietotāja darbā. | 1.1. Datu glabāšana un informācijas apmaiņa.<br><br>(25% no moduļa kopējā apjoma) | 1.1.1. Datu glabāšanas ierīces. | Raksturo datu glabāšanas ierīču veidus, atšķir datu glabāšanas ierīču lietojumu. | Izvērtē un izvēlas datu glabāšanas uzdevumam atbilstošāko datu glabāšanas ierīci. | 10 | 6 | 16 | |
| | | 1.1.2. Datu aizsardzības organizēšanas kārtība. | Organizē datu aizsardzības kārtību. | Izskaidro datu aizsardzības procesu, piedāvā risinājumus datu aizsardzības procesa optimizācijai. | 10 | 6 | 16 | |
| | | 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 glabāšanas ierīci, datu apjomu, kopiju veidošanas biežumu), pārbauda un atjauno datus. | 10 | 6 | 16 | |
| | | 1.1.4. Datu apmaiņa. | Veic drošu datu apmaiņu. | Analizē nepieciešamo datu apmaiņas procesu, piedāvā drošākos risinājumus datu apmaiņai. | 10 | 6 | 16 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2. Spēj: iepazīstināt datorlietotāju ar drošu informācijas glabāšanu.<br><br>Zina: datu glabāšanas un apmaiņas kārtību, datu aizsardzību un iznīcināšanu no neizmantojamiem vai bojātiem datu nesējiem.<br><br>Izprot: drošas informācijas glabāšanas nozīmi datorlietotāja darbā un personas datu aizsardzībā. | 2.1. Datu aizsardzība un droša informācijas glabāšana. (20% no moduļa kopējā apjoma) | 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 informācijas glabāšanas principiem. | Argumentē personas datu aizsardzības nepieciešamību. Raksturo datu apstrādes sistēmas izveidošanas un uzturēšanas noteikumus, izskaidro datorlietotājiem personas datu aizsardzības prasības. | 8 | 6 | 14 | |
| | | **Kopā 6. semestrī:** | | | **48** | **30** | **78** | |
| | | 2.1.2. Privāto datu apdraudējumi un aizsardzība. | Lieto aizsardzības līdzekļus privāto datu drošībai. | Argumentē datu aizsardzības līdzekļu izvēli un izskaidro drošības pasākumu nozīmi. | 8 | 8 | 16 | |
| | | 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 aizsardzībai. | 8 | 8 | 16 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3. Spēj: iepazīstināt datorlietotāju ar ļaundabīgo programmatūru, tās veidiem un izpausmēm.<br><br>Zina: ļaundabīgo programmatūru. veidus, to izpausmes.<br><br>Izprot: ļaundabīgās programmatūras ietekmi uz iekārtas darbu. | 3.1. Ļaundabīgā programmatūra.<br><br>(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. | 8 | 8 | 16 | |
| | | 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. | 12 | 8 | 20 | |
| | | 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. | 8 | 8 | 16 | |
| 4. Spēj: iepazīstināt datorlietotāju ar datorsistēmu un lokālo datortīklu aizsardzību.<br><br>Zina: datu aizsardzības | 4.1. Datorsistēmu un tīklu fiziskā aizsardzība.<br><br>(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. | 8 | 8 | 16 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| nosacījumus, fiziskās vides faktoru ietekmi uz datortehnikas iekārtām un sekas.<br><br>Izprot: datorsistēmu un lokālo tīklu aizsardzības nozīmi to drošai un ilgtspējīgai darbībai. | | 4.1.2. Serveru fiziska aizsardzība (nesankcionēta piekļuve, neatbilstoši klimatiskie apstākļi, ugunsgrēks, plūdi, elektroenerģijas padeves pārtraukumi, tīši bojājumi) | Atpazīst faktorus, kas apdraud datu drošību serveros. Nodrošina datu drošību serveros. | Raksturo datu drošības apdraudējuma faktorus serverī.<br>Piemēro profilakses faktoru riska novēršanai, piedāvā risinājumus drošai datu glabāšanai serverī. | 12 | 8 | 20 | |
| | 4.2. Datorsistēmas un tīklu loģiskā aizsardzība.<br><br>(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. | 12 | 8 | 20 | |
| | | 4.2.2. Ugunsmūris (programmatūras, aparatūras maršrutētājs, bezvadu maršrutētājs). | Nosauc ugunsmūru veidus.<br>Izskaidro aparatūras ugunsmūra nozīmi un iespējas datu drošības uzlabošanai. | Raksturo ugunsmūru veidus.<br>Izskaidro to darbības principus un lietojumu. | 8 | 8 | 16 | |
| | | 4.2.3. Pretvīrusu programmatūra. | Vispārīgi raksturo pretvīrusu programmatūru.<br>Izskaidro uzstādīšanas prasības un atjauninājumu nepieciešamību. Instalē pretvīrusu programmatūru. | Analizē pretvīrusu programmatūras piedāvājumu.<br>Salīdzina antivīrusu programmas un izvēlās piemērotāko. Instalē pretvīrusu programmatūru un veic tās uzturēšanu. | 8 | 6 | 14 | |

| | | | | |
|---|---|---|---|---|
| | **92** | **78** | **170** | |
| **Kopā:** | **140** | **108** | **248** | |

**Moduļa satura īstenošanai izmantojamās metodes:** Prāta vētra, Krustvārdu mīkla, Prezentācija, Diskusija, Patstāvīgais darbs, Mācību ekskursija, Argumentēta eseja, Izpēte, Informācijas tehnoloģiju izmantošana, Darbs ar tekstu.

**Izmantotie avoti:**


Datu aizsardzība [skatīts 2019. gada 1. septembrī]. Pieejams: *hnps:www.esidross.lv/*
Datu drošība [skatīts 2019. gada 1. septembrī]. Pieejams: *hnps:www.cert.lv/*
Drošība tiešsaistē [skatīts 2019. gada 1. septembrī]. Pieejams: *https://ssd.eff.org/en/*
Drošības pasākumi tiešsaistē [skatīts 2019. gada 1. septembrī]. Pieejams: *http://makeitsecure.org/en/index.html*
Informācijas tehnoloģiju drošības likums [skatīts 2019. gada 1. septembrī]. Pieejams: *http://likumi.lv/doc.php?id=220962/*
Lietotāju grupu veidošana Windows vidē [skatīts 2019. gada 1. septembrī]. Pieejams: *http://windows.microsoft.com/lv-lv/windows/user-groups#1TC=windows-7/*
Pretvīrusu programmatūra [skatīts 2019. gada 1. septembrī]. Pieejams: *http://www.pcantivirusreviews.com/Comparison/*
Ugunsmūris [skatīts 2019. gada 1. septembrī ]. Pieejams: *http://computer.howstuffworks.com/firewall.htm*
Vēzis V. Datortīkli un interneta pakalpojumu izmantošana. - Rīga: Mācību grāmata, 2000.


Moduļa programmu izstrādāja skolotājs Jurijs Musatovs