Mācību programma "IT drošības speciālists"

Šī mācību programma paredzēta IT speciālistu tālākizglītībai IT drošības jomā.

Mācību programmas nosaukums	**IKT drošības speciālists**
Apmērs	30 ECTS
Mācību programmas mērķis un sagaidāmie rezultāti	• *informācijas drošības pārvaldības pamatu pārzināšana* • *IT sistēmu drošības nodrošināšanas procesu pielietošana un dalība šo procesu izstrādē un pilnveidošanā* • *pozitīvu biznesa attiecību izveidošana un saglabāšana starp ieinteresētajām pusēm, izmantojot un ievērojot organizatoriskos procesus* • *IT sistēmu droša pārvaldīšana un piedalīšanās šo sistēmu izstrādē un pilnveidošanā*
Moduļi	1. Informācijas drošības pārvaldība - 5 ECTS (HBC) 2. Darbības nepārtrauktības pārvaldība - 5 ECTS (TPT) 3. Pakalpojuma sniegšana - 5 ECTS (TPT) 4. IT risinājumu drošināšana - 15 ECTS (RTK)
Mācību uzsākšanas prasības	Personas, kurām ir EQF 4. līmeņa "IT speciālista" kvalifikācijas kompetence
Mācību pabeigšanas prasības	*Dokumentācija un projektu rezultāti, kas atbilst norādītajiem kritērijiem*

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

1. moduļa ieviešanas plāns:

Nr.	**Moduļa nosaukums**			**Apjoms**
1	Informācijas drošības pārvaldība			**5 ECTS**
Mērķis: Modulis ir izstrādāts, lai veidotu vadības līmeņa izpratni par informācijas drošību un informācijas drošībai pielāgotu uzņēmējdarbības stratēģiju un IKT stratēģiju.				
Moduļa uzsākšanas prasības:				
Sagaidāmie rezultāti	**Vērtēšanas kritēriji**	**Mācību metodes**	**Vērtēšanas metodes un uzdevumi**	**Priekšmets (tēmas, problēmas, temati)**
1. Sniedz ieskatu organizācijas informācijas stratēģijas izstrādē	• Izskaidro informācijas lomu no stratēģiskā viedokļa • Izskaidro stratēģisko savietojumu ar uzņēmējdarbību un IKT stratēģisko konverģenci • Apraksta ekosistēmas kiberdrošību	Lekcijas Projekts / gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "IKT drošības politiku uzlabošanas projekts"	• Informācijas pārvaldība • Informācijas drošības pārvaldība • Drošības modelēšana • Ekosistēmas kiberdrošība • Stratēģiskais savietojums
2. Ievieš organizācijas informācijas stratēģiju	• Pārzina stratēģisko apdraudējumu modelēšanu un saprot informācijas konkurences priekšrocību • Izmanto drošības modelēšanu	Lekcijas Projekts / gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Kiberdrošības, IKT un uzņēmējdarbības stratēģiskais savietojums"	• Stratēģiskais savietojums • Stratēģiskā konverģence • Stratēģiskā apdraudējumu modelēšana un informācijas

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

				konkurences priekšrocība
3. Pārrauga un veic darbības pret ielaušanos, krāpniecību un drošības pārkāpumiem vai informācijas noplūdi	• Izskaidro lomas un ieinteresētās puses informācijas tehnoloģijā • Var veikt vājo vietu un draudu novērtējumu kā darbības ietekmes analīzes daļu • Izskaidro, kā organizācijā saskaņā ar tās drošības dokumentāciju jāpārvalda dati • Var veikt informācijas drošības revīziju	Lekcijas Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Vājo vietu ieviešana un testēšana." Datu pārvaldes plānu un datu klasifikācijas dokumentācija	• Lomas informācijas tehnoloģijā • Vājo vietu novērtējums • Datu pārvalde • Draudu novērtējums • Risku novērtējums • "CIA" triāde- konfidencialitāte, godīgums un pieejamība • Informācijas drošības revīzija
4. Ikdienas darbā ievēro labākās prakses un standartus	• Izskaidro IT pārvaldības labākās prakses, izmantojot kādu plaši pazīstamu satvaru (piem., ITIL) • Izskaidro informācijas drošības pārvaldības standartus (piem., ISO/IEC 27001/27002) • Ikdienas darbā ievēro organizācijas dokumentētās labākās prakses un standartus	Lekcijas Projekts / gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "ISO/IEC 27001/27002 balstītu procesu un procedūru uzlabošana."	• ITIL satvars • ISO/IEC 27001/27002 • Vietējie un starptautiskie tiesību akti

	• Ikdienas darbā ievēro vietējos un starptautiskos tiesību aktus			
Moduļa novērtējums:	Moduļa laikā studenti komandās darbojas ar vairāku veidu dokumentāciju, kurā aprakstītas attiecīgās organizācijas politikas, procedūras un procesi. Studenti saprot organizācijas/uzņēmuma stratēģijas un informācijas stratēģiskās lomas saistību. Komandām jāievieš informācijas drošības politikas, un tās var pārraudzīt un veikt darbības pret visa veida drošības pārkāpumiem. Komandām jāsagatavo darbības nepārtrauktības un ārkārtas atkopšanas darbības. Novērtējums tiek balstīts uz dokumentāciju un laboratorijā veiktā darba iznākumiem, kas tikuši prezentēti. Šī moduļa novērtējums nav sadalošs, studenti būs nokārtojuši moduli, ja visi vērtēšanas kritēriji būs izpildīti vismaz minimālajā nepieciešamajā līmenī.			
Mācību materiāli:				

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

2. moduļa ieviešanas plāns:

Nr.	Moduļa nosaukums			Apjoms
2	**Darbības nepārtrauktības pārvaldība**			**5 ECTS**
Mērķis:	Modulis ir izstrādāts, lai sniegtu studentiem izmaiņu pārvaldības, konfigurācijas pārvaldības un darbības nepārtrauktības pārvaldības pārskatu. Tā ietvaros studenti gūs izpratni par to, kāpēc drošu IT darbību nodrošināšanai nepieciešams pārvaldīt konfigurācijas un izmaiņas.			
Moduļa uzsākšanas prasības:				
Sagaidāmie rezultāti	**Vērtēšanas kritēriji**	**Mācību metodes**	**Vērtēšanas metodes un uzdevumi**	**Priekšmets (tēmas, problēmas, temati)**
1. Nodrošina efektīvu kontroli un programmatūras vai aparatūras izmaiņu plānošanu	• Dokumentē visas instalēšanas laikā veiktās darbības un reģistrē novirzes un koriģējošās darbības • Analizē funkcionālo un tehnisko izmaiņu ietekmi	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Aparatūras un programmatūras izmaiņu plānošana"	• Konfigurācijas pārvaldība • Pakalpojuma objekti un konfigurācijas pārvaldība
2. Minimizē izmaiņu rezultātā radušos pārtraukumu pakalpojumu sniegšanā	• Ievēro atbilstošos drošības standartus un izmaiņu kontroles procedūras, lai saglabātu sistēmas funkcionalitātes un uzticamības integritāti • Ja nepieciešams, sagatavo izmaiņu pieprasījumus • Sniedz ieskatu izmaiņu	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Aparatūras un programmatūras izmaiņu ieviešana"	• Izmaiņu pārvaldība

	pārvaldības procesa pilnveidošanā			
3. Identificē un eskalē iespējamās servisa līmeņa kļūmes un drošības riskus	• Pārliecinās, ka integrētās sistēmas spējas un efektivitāte atbilst specifikācijai • Pārrauga drošības vadību • Analizē uzņēmuma nozīmīgos objektus un identificē *draudus*, trūkumus un vietas, kuras nav pilnībā aizsargātas pret ielaušanos vai uzbrukumu	Lekcijas Lasīšana Diskusija grupās Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Vājo vietu novērtējums"	• Jaudas pārvaldība • Vājo vietu pārvaldība
4. Nodrošina, ka tiek analizēti un pārvaldīti drošības riski uzņēmuma datu un informācijas jautājumos	• Veic riska pārvaldības revīzijas un rīkojas, lai minimizētu risku • Izstrādā vai uzlabo riska pārvaldības plānu, lai identificētu nepieciešamās profilakses darbības	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Riska pārvaldība"	• Riska pārvaldība
5. Pārvalda darbības nepārtrauktības un ārkārtas atkopšanas plānus	• Piedalās ārkārtas atkopšanas darbības nepārtrauktības plānu izstrādes un pārvaldes procesos • Validē ārkārtas atkopšanas plānu, lai nodrošinātu, ka tas ir atjaunināts un atbilst realitātei	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Darbības nepārtrauktības plāns un ārkārtas atkopšanas plāns."	• Ārkārtas atkopšanas plāns • Darbības nepārtrauktības plāns • Plānošanas process

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

Moduļa novērtējums:	Moduļa laikā studenti komandās darbojas ar vairāku veidu projektiem, kas saistīti ar konfigurācijas pārvaldību, izmaiņu pārvaldību un darbības nepārtrauktības pārvaldību. Studenti gūst izpratni par saistību starp organizācijas/uzņēmuma pakalpojumu uzticamību un nepieciešamību nodrošināt, ka visas izmaiņas tiek rūpīgi dokumentētas. Komandām jāsagatavo īsta konfigurācijas pārvaldības datubāze, izmaiņu pārvaldības risinājums un jāizstrādā un jātestē ārkārtas atkopšanas plāns. Šī moduļa novērtējums nav sadalošs, studenti būs nokārtojuši moduli, ja minimālajā nepieciešamajā līmenī būs izpildīti visi vērtēšanas kritēriji.			
Mācību materiāli:				

3. moduļa ieviešanas plāns:

Nr.	**Moduļa nosaukums**			**Apjoms**
3	**Pakalpojuma sniegšana**			**5 ECTS**
Mērķis:	Modulis ir izstrādāts, lai sniegtu studentiem pakalpojuma sniegšanas procesa pārskatu. Šajā modulī lielākā uzmanība pievērsta incidentu pārvaldībai, problēmu pārvaldībai un klientu atbalstam.			
Moduļa uzsākšanas prasības:				
Sagaidāmie rezultāti	**Vērtēšanas kritēriji**	**Mācību metodes**	**Vērtēšanas metodes un uzdevumi**	**Priekšmets (tēmas, problēmas, temati)**
1. Atbild uz lietotāju prasībām un problēmām, reģistrējot atbilstošu informāciju un nodrošinot atrisinājumu vai eskalējot incidentus	• Izmanto atbalsta rīkus, lai sistemātiski izsekotu kļūdas vai tehniskas kļūmes avotu • Analizē simptomus, lai identificētu lietotāja kļūdas vai tehniskas kļūmes aptuveno veidu • Eskalē sarežģītus vai neatrisinātus incidentus	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Diskusija: "Kas ir incidents, problēma un kļūme?" Projekta darbs un dokumentācija: "Incidentu pārvaldība IT organizācijā"	• Incidentu pārvaldība • Klientu pārvaldība
2. Identificē un novērš incidentu pamatcēloni	• Identificē un klasificē incidentu veidus un traucējumus pakalpojuma sniegšanā • Identificē iespējamas kritiskas komponentu kļūmes un veic darbības, lai mazinātu kļūmes efektus	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Incidentu pamatcēloņu atrašana"	• Incidentu klasifikācija • Problēmu pārvaldība

3. Nosaka dokumentācijas prasības, ņemot vērā tam piemēroto mērķi un vidi	• Uz visu dzīves ciklu saglabā risinājumam pielīdzinātu dokumentāciju • Nodrošina, ka organizācijas drošības dokumentācija ir atjaunināta	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Organizācijas zināšanu bāzes izstrādāšana"	• Dokumentu pārvaldība • Dokumentu pārvaldības sistēmas • Zināšanu pārvaldības sistēmas
4. Nodrošina, ka ieinteresēto pušu vajadzības, bažas un sūdzības tiek izprastas un risinātas saskaņā ar organizatorisko politiku	• Saprot klientu vajadzības • Ziņo citiem departamentiem par drošības prasībām • Izskaidro drošības darbību nepieciešamību	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Lomu spēle: "Komunikācija ar tiešo lietotāju" Projekta darbs un dokumentācija: "Komunikācijas sistēmas izveidošana ar drošību saistītiem paziņojumiem"	• Klientu atbalsts • Komunikācijas pārvaldība
5. Izseko uzticamības un veiktspējas datus un salīdzina tos ar PLL	• Uztur pārraudzības un pārvaldes rīkus • Analizē pakalpojuma sniegšanas nodrošināšanu un ziņo vecākajiem kolēģiem par iznākumu	Lekcijas Lasīšana Diskusija grupā Projekts laboratorijā/ gadījumu izpēte Prezentācija	Projekta darbs un dokumentācija: "Lietotņu veiktspējas pārvaldība"	• Sistēmu pārraudzība • Drošības pasākumu pārvaldība • Pakalpojuma sniegšanas pārvaldība
Moduļa novērtējums:	Moduļa laikā studenti komandās darbojas ar vairāku veidu projektiem, kas saistīti ar incidentu pārvaldību, problēmu pārvaldību un klientu atbalstu. Studenti gūst izpratni par saistību starp organizācijas/uzņēmuma pakalpojumu un laba klientu atbalsta nepieciešamību un saprot, ka visus incidentus un problēmas rūpīgi jādokumentē. Studenti var izskaidrot drošības darbību nepieciešamību. Komandām jāsagatavo īsts incidenta pārvaldības risinājums ar zināšanu pārvaldības sistēmas atbalstu, tādējādi			

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

	palīdzot samazināt klientu atbalsta dienesta darba slodzi. Šī moduļa novērtējums nav sadalošs, studenti būs nokārtojuši moduli, ja minimālajā nepieciešamajā līmenī būs izpildīti visi vērtēšanas kritēriji.
Mācību materiāli:	

4. moduļa ieviešanas plāns:

Nr.	Moduļa nosaukums			Apjoms
4	IT risinājumu drošināšana			15 ECTS
Mērķis:	Modulis ir izstrādāts, lai mācītu un sniegtu praktiskas iemaņas studentiem IT risinājumu drošības jomā. Tajā ietverti droši datortīklu risinājumi; serveru, darbstaciju un mobilo ierīču drošība; ārkārtas atkopšanas un mākoņdatošanas risinājumu drošība.			
Moduļa uzsākšanas prasības:	EQF 4. līmeņa kvalifikācijas kompetences IKT jomā (piem., Datorsistēmu tehniķis).			
Sagaidāmie rezultāti	**Vērtēšanas kritēriji**	**Mācību metodes**	**Vērtēšanas metodes un uzdevumi**	**Priekšmets (tēmas, problēmas, temati)**
1. Ieviešdrošus datortīklu risinājumus	• Apraksta uz tīklu risinājumiem vērstu iespējamo uzbrukumu veidus • Pārzina pamata kriptogrāfijas paņēmienus • Ievieš datortīklos kriptogrāfijas paņēmienus, algoritmus un lietotnes • Ievieš aparatūras un programmatūras risinājumus, lai novērstu OSI modeļa un datortīkla vājās vietas • Nodrošina bezvadu tīklu aizsardzību, izmantojot "šifrēšanas" un "paroles" sistēmas • Ja nepieciešams, šifrē tīkla	Lekcija Diskusija grupā Prakse Video lekcija Lasīšana Prezentācija	• Praktiskais darbs grupās: "OSI modeļa slāņu drošības risinājumi" • Tests: "OSI modeļa drošības risinājumi" • Prezentācija: "Uz bezvadu tīkliem vērstu uzbrukumu veidi" • Tests: "Uz datortīkliem vērstu uzbrukumu veidi" • Praktiskais darbs: "Attiecīgās datortīkla diagrammas priekšrocības un vājās vietas" • Prezentācija: "Dažādu tīkla aprīkojumu aizsardzība pret neatļautu piekļuvi"	• OSI modeļa izstrādes principi • Svarīgākās ar OSI modeli saistītās problēmas • Aizsardzība pret uzbrukumiem, kas izmanto OSI modeļa vājās vietas • IP un MAC filtri, IP adrešu piešķiršana, drošība • Bezvadu tīklu drošība • Aizsardzība pret uzbrukumiem datortīkliem un telesakaru sistēmām • Pamata kriptogrāfijas paņēmieni. Šifrēšanas veidi, to izmantojums droša savienojuma

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

	savienojumus • Pārrauga datortīkla darbību, izmantojot dažādas lietotnes		• Praktiskais darbs: "Tīkla ierīču drošināšana" • Praktiskais darbs: "Tīkla risinājuma drošināšana"	izstrādē • Uz datortīkliem vērstu uzbrukumu klasifikācija
2. Droši pārvalda darbstacijas un mobilās ierīces	• Pārvalda darbstacijas, izmantojot domēna kontrollera risinājumus • Noslēdz darbstacijas, lai nodrošinātu to drošību • Ievieš domēnu drošības politikas un iedala darbstacijas drošības grupās • Ievieš sinhronizāciju, datu drošību dažādās mobilajās ierīcēs un darbstacijās	Lekcija Projekta darbs Lasīšana Prezentācija	• Tests – "Darbstacijas drošība – klienta puse" • Praktiskais darbs - "Darbstaciju stiprināšana" • Praktiskais darbs - "Mobilās ierīces drošība"	• Darbstaciju noslēgšanas risinājumi • Centrālā darbstaciju pārvalde • Lietotājatkarīga drošība • Mobilās ierīces drošība
3. Piemēro drošības politikas, lai nodrošinātu servera drošību	• Servera drošībai konfigurē ugunsmūri • Nodrošina DNS un DHCP serveru aizsardzību. • Nodrošina e-pasta un tīmekļa serverus • Pārvalda VPN politiku. • Ievieš AAA modeli i. Autentificēšana; ii. Licencēšana; iii. Uzskaite. • Ievieš serverī diska šifrēšanu	Lekcija Projekta darbs Lasīšana Prezentācija	• Praktiskais darbs: "Grupas politika" • Praktiskais darbs: "DHCP un DNS aizsardzība" • Praktiskais darbs: "E-pasta servera drošināšana" • Praktiskais darbs: "Tīmekļa servera drošināšana" • Tests - "Ugunsmūris un VPN politika" • Praktiskais darbs: "AAA	• Ugunsmūra konfigurēšana servera drošībai. • DNS un DHCP – iespējamās drošības problēmas un to risinājumi. • Tīmekļa serveru drošināšana • VPN – konfigurēšana un politika. • E-pasta un tīmekļa serveru drošināšana • Autentificēšana, licencēšana un uzskaite,

			ieviešana un drošība direktorija pakalpojumā“ • Praktiskais darbs: "Attālās piekļuves drošināšana serverim"	izmantojot direktorija pakalpojumus • Diska šifrēšanas risinājums uzņēmuma tīklā • Droša attālā piekļuve serverim
4. Droši izmanto mākoņrisinājumus	• Saprot mākoņdatošanas tehnoloģiju izmantošanu datu pārraides aizsardzībā • Saprot mākoņdatošanas pakalpojumu sniedzēju savienojuma drošību • Spēj sadarboties ar mākoņdatošanas pakalpojumu sniedzējiem	Lekcija Video lekcija Prezentācija	• Komandas darbs: "Mākoņdatošanas pakalpojumu sniedzēju savienojuma aizsardzība" • Praktisks uzdevums: "Mākoņdatošanas izmantošana IT sistēmas drošināšanā"	• Mākoņdatošanas tehnoloģijas • Mākoņdatošanas pakalpojumu sniedzēji un pakalpojumu veidi • Mākoņdatošanas pakalpojumu savienojuma drošību
5. Ievieš ārkārtas atkopšanas un dublējuma risinājumus	• Konfigurē failu dublēšanas pakalpojumu • Automatizē failu dublējumu uzglabāšanu vietējā vai globālā tīklā. • Aizsargā dublējumserverus pret neatļautu izmantošanu. • Spēj testēt un atjaunot izveidotu dublējumu	Lekcija Video lekcija Lasīšana Prezentācija	• Praktisks uzdevums: "Dublējuma failu izveidošana un uzglabāšana" • Praktisks uzdevums: "Tīkla aprīkojuma konfigurācijas dublējuma nodrošināšana" • Praktisks uzdevums: "Dublējuma failu aizsardzība" • Praktisks uzdevums:	• Dublējuma risinājumi un dublējuma failu veidi • Dublēšanas automatizēšana. • Dublējuma risinājumu aizsardzība • Aprīkojuma pārraudzības dublējums • Ārkārtas atkopšana – dublējumu atjaunošana • Dublējuma risinājuma testēšana

			"Dublējuma atjaunošana" • Praktisks uzdevums: "Dublējuma atjaunošanas testēšana"	
Moduļa novērtējums:	Moduļa novērtējums ir atkarīgs no kopējā snieguma katrā uzdevumā. Students spēj nodrošināt un pārvaldīt IT risinājumus uzņēmumā (darbstacijas, serverus, mākoņdatošanas risinājumus, tīkla infrastruktūru), kā arī ieviest un aizsargāt IT ārkārtas atkopšanas risinājumus. Šī moduļa novērtējums nav sadalošs, studenti būs nokārtojuši moduli, ja minimālajā nepieciešamajā līmenī būs izpildīti visi vērtēšanas kritēriji.			
Mācību materiāli:				

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund

Profesijas standarta kompetenču un mācību programmas moduļu salīdzinājums

Moduļi/kompetences	B.2.1. **IKT risinājumu izstrāde**	B.2.2. **Tehnoloģiju attīstības tendenču pārraudzīšana**	B.2.3. **Komponentu integrācija**	B.2.4. **Testēšana**	B.2.5. **Risinājumu izvietošana**	B.2.6. **Dokumentācijas izstrāde**	B.2.7. **Lietotāju atbalsts**	B.2.8. **Atbalsts izmaiņu gadījumā**	B.2.9. **Pakalpojuma sniegšana**	B.2.10. **Problēmu pārvaldība**	B.2.11. **Informācijas drošības stratēģijas izstrāde**	B.2.12. **Personāla attīstība**	B.2.13. **Riska pārvaldība**	B.2.14. **Attiecību pārvaldība**	B.2.15. **Informācijas drošības pārvaldība**
Informācijas drošības pārvaldība (1)		X				X		X			X	X	X	X	X
Darbības nepārtrauktības pārvaldība (2)		X				X		X	X	X				X	X
Klientu apkalpošana / Pakalpojuma sniegšana (3)		X				X	X							X	
IT risinājumu drošināšana (4)	X	X	X	X	X	X	X		X			X	X	X	

Interreg Central Baltic

EUROPEAN UNION
European Regional Development Fund