



Mācību programma Kiberdrošības speciālista profesionālā pilnveide

Programma “Kiberdrošības speciālista prakse” paredzēta publiskās pārvaldes kiberdrošības speciālistiem, kuri vēlas sistemātiski attīstīt praktiskās un teorētiskās iemaņas informācijas sistēmu aizsardzībā un drošības pārvaldībā. Mācību laikā apgūsi, kā atpazīt un novērtēt kiberdrošības riskus, ieviest efektīvus aizsardzības pasākumus un nodrošināt tehnoloģisko resursu drošības prasības.

Īpašs uzsvars likts uz praktiskajām prasmēm – dalībnieki trenēsies konfigurēt drošības risinājumus, strādāt ar kriptogrāfijas atslēgām, pārvaldīt piekļuves politikas, izmantot dažādus autentifikācijas mehānismus, kā arī darboties ar SIEM/XDR sistēmām incidentu izmeklēšanai. Pēc mācību programmas apguves dalībnieki spēs efektīvi reaģēt uz apdraudējumiem, pielietot atbilstošus aizsardzības rīkus un sniegt ieguldījumu iestādes kopējā kiberdrošības stiprināšanā.

Formāts

Jaukta tipa: klātienēs un tiešsaistes lekcijas

Kāpēc piedalīties?

Kiberdrošības speciālista loma publiskajā pārvaldē prasa ne tikai teorētiskas zināšanas, bet spēju rīkoties reālās situācijās – savlaicīgi, droši un profesionāli. Šī programma sniedz praktisku pieredzi darbā ar mūsdienīgiem drošības risinājumiem, incidentu scenārijiem un aktuālo kiberdraudu vidi, kas tieši ietekmē valsts informācijas sistēmu drošību.

Mācības vada TET kiberdrošības speciālisti ar plašu praktisko pieredzi, ikdienā strādājot ar sarežģītiem drošības izaicinājumiem, infrastruktūrām un incidentiem. Dalībniekiem tā ir iespēja mācīties no nozares profesionāļiem, iegūt praktiski pielietojamas zināšanas un stiprināt savu kompetenci infrastruktūras aizsardzībā, drošības uzraudzībā un incidentu reaģēšanā. Programma palīdz ne tikai attīstīt individuālās prasmes, bet arī sniegt reālu ieguldījumu iestādes kiberdrošības noturības stiprināšanā.

Programmas mērķis

Nodrošināt kiberdrošības speciālistus ar praktiskām zināšanām un prasmēm, kas nepieciešamas, lai uzturētu un aizsargātu organizācijas IT infrastruktūru, identificētu un novērstu drošības apdraudējumus, kā arī reaģētu uz incidentiem, ievērojot labās prakses un saistošos normatīvos regulējumus.

Mērķauditorija

Publiskajā pārvaldē nodarbinātie kiberdrošības speciālisti un citu lomu pārstāvji atbilstoši to attīstības vajadzībām.

Programmas moduļi

1. IKT resursu identificēšana, uzskaitē un klasifikācija kiberdrošības kontekstā;
2. Kiberdrošības draudi, riski un aktuālās aizsardzības stratēģijas;
3. Drošības arhitektūras principi un drošības risinājumu ieviešana iestādes infrastruktūrā;
4. Serveru, tīklu, lietotāju un mākoņvides drošības konfigurācija;
5. Tīklu drošība, ugunsūmuri, VPN un citi aizsardzības risinājumi;
6. Sistēmu noturība, darbības nepārtrauktība un rezerves kopēšana;
7. Drošības uzraudzība, SIEM/XDR izmantošana un incidentu analīze;
8. Kiberdrošības incidentu atklāšana, reaģēšana un dokumentēšana

Nosacījumi dalībai

Nepieciešamās priekšzināšanas:

- Vidējā profesionālā vai augstākā izglītība IT jomā vai līdzvērtīga darba pieredze.
- Labas zināšanas par tīklu darbību.
- Pieredze serveru administrēšanā (Windows/Linux).
- Digitālās pamatprasmes (dokumentu apstrāde, attālinātas sadarbības platformas).
- Klātienēs nodarbībās nepieciešams savs dators.



Programmas ieguvumi

- Praktiskas, darbā uzreiz pielietojamas kiberdrošības prasmes.
- Padziļināta izpratne par aktuālajiem kiberdraudiem un riskiem publiskajā pārvaldē.
- Pieredze darbā ar drošības uzraudzības un SIEM/XDR risinājumiem.
- Prasme atklāt, analizēt un dokumentēt kiberdrošības incidentus.
- Zināšanas sistēmu noturības un darbības nepārtrauktības nodrošināšanā.
- Iespēja mācīties no TET kiberdrošības speciālistiem ar praktisku pieredzi nozarē.

Pasniedzēji – nozares vadošie eksperti



Uldis Lībietis

Kiberdrošības nozares profesionālis ar vairāk nekā septiņu gadu praktisku pieredzi kiberdrošības pārvaldībā un operatīvajā darbā. Ikdienā strādā SIA TET kā Datu aizsardzības un IT risku nodaļas vadītājs, nodrošinot kiberdrošības risku vadību, incidentu pārvaldību un atbilstību ISO 27001, PCI-DSS un normatīvo aktu prasībām. Viņam ir arī praktiska pieredze kiberdrošības pārvaldībā valsts un pašvaldību iestādēs. U.Lībietis ikdienā darbojas ar SIEM/XDR risinājumiem, infrastruktūras aizsardzību, incidentu analīzi un reaģēšanu. Papildus praktiskajam darbam Uldim Lībietim ir vairāku gadu pieredze mācību vadīšanā akadēmiskajā un profesionālajā vidē, īpašu uzsvaru liekot uz praktiski pielietojamām zināšanām un reāliem scenārijiem.



Gatis Polis

Kiberdrošības un IKT risku pārvaldības speciālists ar praktisku pieredzi. Viņa profesionālā darbība ietver kiberdrošības risku novērtēšanu, drošības politiku ieviešanu un incidentu pārvaldību atbilstoši nacionālajam un starptautiskajam regulējumam. Strādājot SIA TET, viņš ikdienā nodrošina MK Nr. 397 prasību ieviešanu, drošības kontroles pasākumu uzraudzību un organizāciju noturības stiprināšanu. Gatis Polis praktiski darbojas ar drošības notikumu uzraudzību un infrastruktūras aizsardzības jautājumiem. Papildus tam viņam ir plaša pieredze kiberdrošības mācību vadīšanā dažādām auditorijām, īpašu uzmanību pievēršot kiberhigiēnai, risku izpratnei un drošai rīcībai ikdienas darbā.

[Pieteikties](#)

Mācību programma

Datums	Klātienē/ Tiešsaistē	Tēma	Lektors/-e
1. modulis IKT resursi un kiberdrošības riski			
02.02.2026. 09.00-12.15	Tiešsaistē	- IKT resursu identificēšanas un uzskaites pamati un pielietojamie risinājumi - IKT resursu klasifikācija - Drošības draudu modelēšana un klasifikācija (piem., ārējie, iekšējie, fiziskie, digitālie) - Risku izvērtēšana un līmeņa noteikšana - Risku mazinošo pasākumu plānošana un uzraudzība	Uldis Lībietis
04.02.2026. 09.00-13.45			
2. modulis Aktuālās kiberdrošības tendences			
05.02.2026. 10.45-15.30	Tiešsaistē	- Modernie kiberdraudi (APT, ransomware, phishing 2.0 u.c.) - Dažādas drošības aizsardzības stratēģija (Zero Trust, Defense in Depth, Risk-based security, MI drošībā u.c.) - Kiberdrošības aktualitāšu ieguves avoti un to praktiskie pielietojumi - CVD procesa tvērums - Piegādes ķēžu uzbrukumi	Gatis Polis
3. modulis Drošības arhitektūra un risinājumu integrācija			
05.02.2026. 09.00-10.30	Tiešsaistē	Izprast drošības arhitektūru kopējo konceptu skatā no augšas (tīklu drošība, serveru drošība, iekārtu drošība, lietotāju pārvaldība un monitoringa iespējas)	Gatis Polis un eksperts Kristaps Kūlis
4. modulis Drošības risinājumi un administrēšana			
Attālināti 10.02.2026. 09.00-12.15 12.02.2026. 13.00-16.15 Klātienē 16.02.2026. 09.00-16.15 Attālināti 18.02.2026. 09.00-12.15	Attālināti un viena klātienes nodarbība	- Windows un Linux serveru un gala iekārtu drošības iestatījumi; - Centralizēta drošības pārvaldība Windows vidē (GPO un Intune); - Paroļu politika, MFA, SSH un citu sertifikātu pārvaldība un piekļuves kontrole; - Populārāko servisu drošības risinājumu un to konfigurācija un izmantošanas iespējas (WEB, DB, E-pasta sistēmas, DNS u.c.); - Mākoņpakalpojumu drošības konfigurācija (kontu drošība, drošības modelis, nosacījuma pieejas tiesību, administrācija balstoties uz lomām u.c.); - Virtualizācijas un konteinerizācijas drošības iestatījumi (Hypervisor, VM un Konteineri); “CIS benchmarks” materiāli.	Gatis Polis un eksperts Kristaps Kūlis
19.02.2026. 09.00-12.15 20.02.2026. 09.00-12.15 20.02.2026. 13.00-16.15	Tiešsaistē	- Drošas tīkla arhitektūras principi; - Ugunsmūru veidi; - Ugunsmūra – drošības iestatījumi un politikas izstrāde; - IDS/IPS un WAF pielietojums; - VPN veidi un konfigurācija.	Gatis Polis un eksperts Māris Zunde

Mācību programma

Datums	Klātienē/ Tiešsaistē	Tēma	Lektors/-e
5. modulis Infrastruktūras uzturēšana un nepārtrauktības nodrošināšana			
27.02.2026. 13.00-16.15	Tiešsaistē	- NDP infrastruktūras risku izvērtēšana; - NDP plānošana un kritēriju noteikšana, kā RTO, RPO un MTD.	Gatis Polis
02.03.2026. 13.00-14.30 04.03.2026. 13.00-16.15		- RK dokumentācijas un stratēģijas (pilns, inkrementāls, diferenciāls) izpratne, izvēle un pielietojums; - RK uzglabāšanas kritēriji un to nodrošināšana; - RK testēšana un atjaunošana; - Reāllaika sistēmu datu konsekvence sasaistē ar rezerves kopijām.	
6. modulis Drošības uzraudzības un pārvaldība			
05.03.2026. 13.00-16.15 06.03.2026. 10.45-14.30 10.03.2026. 13.00-16.15	Tiešsaistē	- Monitoringa un uzraudzības rīki (Zabbix, Grafana, u.c.); - Centralizēti logošanas risinājumi; - SIEM/XDR risinājumu iespējas.	Uldis Lībietis un eksperts Rolands Bīrons
09.03.2026. 09.00-16.15	Klātiene	- Integrācija ar esošajām sistēmām (IAM, DLP, MDM); - Sadarbība ar izstrādātājiem un sistēmanalītiķiem.	Uldis Lībietis
7. modulis Kriptogrāfijas loma un lietojums			
11.03.2026. 09.00-12.15	Tiešsaistē	- Kriptogrāfijas loma un lietojums kiberdrošībā (VPN, Rezerves kopijas, TLS savienojumi u.c.) - PGP izmantošanas principi	Gatis Polis
8. modulis Incidentu atklāšana un reaģēšana			
11.03.2026. 13.00-16.15	Attālināti	- Savu iekārtu uzraudzība ārējā un iekšējā tīklā - Servisu un programmatūras versiju kontrole un pārraudzība	Uldis Lībietis un eksperts Rolands Bīrons
13.03.2026. 10.45-15.30 17.03.2026. 10.45-15.30 19.03.2026. 10.45-14.30	Tiešsaistē	- SIEM/XDR sistēmu lietojums (Splunk, ELK, Sentinel u.c.) - Žurnālfailu analīze, anomāliju identificēšana - Kompromitācijas indikatori (IoC)	Uldis Lībietis un eksperts Rolands Bīrons
23.03.2026. 10.45-15.30 24.03.2026. 10.45-15.30	Tiešsaistē	- Incidentu atklāšana, klasifikācija un prioritizēšana - Incidentu reaģēšanas plāni - Incidentu dokumentēšana un ziņošana - Sadarbības organizēšana incidenta novēršanā	Gatis Polis