Valsts policijas koledža

|  |  |  |  |
| --- | --- | --- | --- |
| Programmas nosaukums | | **Ar elektroniskās informācijas sistēmām izdarītu noziedzīgu nodarījumu kvalifikācija un izmeklēšana** | |
| Programmas mērķis  Programmas mērķauditorija  Klausītāju skaits  Programmas īstenošanas ilgums | | **pilnveidot Valsts policijas amatpersonu, kuras veic izmeklēšanu kriminālprocesos par noziedzīgiem nodarījumiem kibernoziegumu jomā, zināšanas par noziedzīgu nodarījumu kvalifikāciju, izmeklēšanas īpatnībām, pierādāmiem apstākļiem, par elektronisko pierādījumu ieguvi, starptautiskās sadarbības pasākumu īstenošanu**  **Valsts policijas amatpersonas, kuras veic izmeklēšanu kriminālprocesos par noziedzīgiem nodarījumiem kibernoziegumu jomā**  **līdz 20**  **8 akadēmiskās stundas** | |
| Programmas izstrādātājs | | **Mg. iur. Dainis Šteinbergs, Valsts policijas koledžas Tiesību zinātņu katedras lektors** | |
| Izglītības dokuments, kas apliecina  profesionālās izglītības programmas apguvi | | **apliecība** | |
| Nosacījumi dokumenta, kas apliecina programmas apguvi, saņemšanai | | **klausītājs, piedaloties programmas apguvē vismaz 90% apmērā, saņem apliecību** | |
| Programmas izstrādes gads | | **2019** | |
| Programmas plāns | |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr.p.k. | Laiks | Tēmas nosaukums | Taksonomijas  līmenis | Akadēmisko stundu skaits | | | Izmantojamās  metodes | Pedagogs |
| Teorija | Prakt. darbs | Kopā |
| 1. | 10.00 –  11.30 | Krimināllikumā ietverto noziedzīgo nodarījumu, kuri var tik veikti, izmantojot elektroniskās informācijas sistēmas, vispārīgais raksturojums. | izpratne un pielietojums | 2 | - | 2 | lekcija un diskusija | D.Šteinbergs |
| 2. | 11.30  -  12.45 | 2.1.Informācijas sistēmu drošība, ar to saistītie pamatjautājumi un reglamentējošie juridiskie akti.  2.2.Kibernoziegumu kvalifikācijas īpatnības. | izpratne un pielietojums | 1 | - | 1 | lekcija un diskusija | D.Šteinbergs |
| 3. | 12.45  -  15.00 | 3.1.Elektroniskie pierādījumi kriminālprocesā:  3.1.1.elektronisko pierādījumu jēdziens, to krimināl-procesuālais raksturojums;  3.1.2.elektronisko pierādījumu iegūšanas principi kriminālprocesā;  3.1.3.elektroniskās informācijas sistēmā esošu datu saglabāšanas kriminālprocesuālais raksturojums un starptautiskais regulējums;  3.1.4.elektroniskajā informācijas sistēmā saglabāto datu atklāšanas un izsniegšanas pamats nacionālajā un starptautiskajā tiesiskajā regulējumā.  3.2.Eiropas Cilvēktiesību prakse par sistēmās esošu datu saglabāšanu. | izpratne un pielietojums | 2 | 1 | 3 | lekcija, diskusija  un  praktisks uzdevums | D.Šteinbergs |
| 4. | 15.00  -  16.30 | 4.1.Starptautiskā sadarbība elektronisko pierādījumu iegūšanā:  4.1.1.iespējamie veidi elektronisko pierādījumu iegūšanā no ārvalstīm;  4.1.2.elektronisko pierādījumu pieprasīšanas no ārvalstīm procedūra.  4.2.Informācijas pieprasīšana no ārvalstu pakalpojumu sniedzējiem. | izpratne un pielietojums | 2 | - | 2 | lekcija un diskusija | D.Šteinbergs |
|  |  |  | **KOPĀ** | **7** | **1** | **8** |  |  |

|  |  |
| --- | --- |
| Izmantojamās literatūras un avotu saraksts: | * 1. Latvijas Republikas Satversme;   2. likums “Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās:   3. 2001.gada 23.novembra Konvencija par kibernoziegumiem un Konvencijas par kibernoziegumiem 2003.gada 28.janvāra Papildu protokols;   4. Eiropas Padomes 1995.gada 11.septembra dokuments „Par rekomendācijām procesuālajās tiesībās, kas saistītas ar informācijas tehnoloģiju izmantošanu” (R(95)13 Problems of criminal procedural law connected with information technology);   5. Krimināllikums;   6. Kriminālprocesa likums;   7. Elektronisko sakaru likums;   8. Valsts informācijas sistēmu likums;   9. Ministru kabineta 2007.gada 4.decembra noteikumi Nr.820 „Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu”;   10. Ministru kabineta 2014.gada 6.augusta rīkojums Nr.416 “Par Eiropas Parlamenta un Padomes Direktīvā 2013/40/ES (2013.gada 12.augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI, paredzētā kontaktpunkta noteikšanu”;   11. Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija, Rīga, Jumava, 2015;   12. Ķinis U. Noziedzīgi nodarījumi pret informācijas sistēmu drošību. Kibernoziegumi. Rīga, Turība, 2007;   13. Brenner S. W., Cybercrime. Criminal threats from cyberspace. Praeger, 2010;   14. Russel G. Smith, P. Grabovsky, Gregor Urbas, Cybercriminals on trial, Cambridge University press, 2004;   15. Kerr O. Computer crime law, Thomson and west;   16. <http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/PR/2017/05-29/1125764LV.pdf>;   17. Eiropas Parlamenta un Padomes direktīva 2013/40/ES, pieejama: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32013L0040>;   18. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>. |

ŠIS DOKUMENTS IR PARAKSTĪTS AR ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU