**DAUGAVPILS UNIVERSITĀTES**

**STUDIJU KURSA APRAKSTS**

|  |  |
| --- | --- |
| Studiju kursa nosaukums | ***Kiberdrošības pamati un personu un uzņēmumu informatīvā drošība*** |
| Studiju kursa kods (DUIS) |  |
| Zinātnes nozare | #Datorzinātne |
| Kursa līmenis |  |
| Kredītpunkti | 6 |
| ECTS kredītpunkti | 9 |
| Kopējais kontaktstundu skaits | 96 |
| Lekciju stundu skaits | 64 |
| Semināru stundu skaits | 16 |
| Praktisko darbu stundu skaits | 16 |
| Laboratorijas darbu stundu skaits |  |
| Studējošā patstāvīgā darba stundu skaits | 144 |
|  | |
| Kursa autors(-i) | |
| Mg.sc.comp., lekt. Andrejs Radionovs | |
| Kursa docētājs(-i) | |
| Mg.sc.comp., lekt. Andrejs Radionovs  Dr.iur., asoc.prof. Aleksandrs Matvejevs | |
| Priekšzināšanas | |
|  | |
| Studiju kursa anotācija | |
| Kursa mērķis – iepazīstināt studējošos ar jaunākajām digitālo tehnoloģiju tendencēm, kiberdrošību, veidojot studējošajiem izpratni par personu un uzņēmumu informatīvo drošību un tās tiesisko nodrošinājumu, kā arī sagatavot speciālistus ar padziļinātām zināšanām informācijas sistēmu un datortīklu aizsardzībā pret kiberuzbrukumiem.  Kursa uzdevumi:  - iepazīstināt studējošos ar jaunākajām attīstības tendencēm un kiberdrošību;  - iemācīt studējošos drošam darbam ar digitālām tehnoloģijām;  - iepazīstināt studējošos ar Eiropas un Latvijas Republikas normatīviem dokumentiem, kuri aizsargā cilvēku personīgo informāciju un regulē IKT drošību;  - pilnveidot zināšanas par IKT drošības riskiem (t.sk. mūsdienu datortīklos, mobilās platformās, mākoņsistēmās un citur) un to mazināšanas paņēmieniem;  - iepazīstināt studējošos ar dažādam aizsardzības sistēmām, kā digitālam, tā arī fiziskam (t.sk. videonovērošanas sistēmām);  - attīstīt prasmes izvelēties konkrētus aizsardzības mehānismus un argumentēt to izvēli;  - veidot kompetenci praktiskai datortīklu aizsardzības mehānismu realizēšanai.  - attīstīt prasmi strādāt ar literatūras avotiem, kurus izmanto IT industrijā, nozares vadlīnijas un standartus, un pamatot savus lēmumus uz tiem. | |
| Studiju kursa kalendārais plāns | |
| Kursa struktūra: lekcijas – 64 st., seminārs - 16 st. praktiskie darbi - 16 st.  1. IKT drošības pamatprincipi, kiberdrošība. (L2)  2. Netiķete. (S2)  3. Kiberdrošība gan darbā gan mājas. (S2)  4. Iekšējie datu apstrādes aizsardzības noteikumi. (L2)  5. Informācija, kā tiesiskās aizsardzības objekts. (S2)  6. Vispārīgā datu aizsardzības regula. (L4)  7. Personas datu aizsardzības jēdziens, personas datu apstrādes principi un mērķi. (L4)  8. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība. (L4)  9. Personas datu aizsardzības speciālista funkcijas un pienākumi. (L2)  10. Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums. (L2)  11. Kriminālatbildība un administratīvie pārkāpumi informatīvās drošības jomā. (S2)  12. Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. (L4)  13. Nesankcionēta piekļuve informācijai, sociālā inženierija, konfidencialitāte. (S4)  14. CSRF, XSS uzbrukumi, SQL injekcijas. (L4)  15. Sociālā inženierija, netieši un rupja spēka uzbrukumi (CSRF, XSS uzbrukumi un SQL injekcijas). (P2)  16. Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. (L4)  17. Videonovērošanas un telpu piekļuves kontroles sistēmas. (L4) )(P2)  18. Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti. (L4)  19. Drošības pasākumu plānošana, risku analīze. (S2)  20. Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati. (L4)  21. Informācijas sistēmu drošības audits. (P2)  22. Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. (L2)  23. Personu un uzņēmumu īpašuma apdraudējuma veidi tīklā. (S2)  24. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes. (L4)  25. Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. (L2) (P2)  26. Interneta protokolu drošība, TCP, DNS un maršrutēšana. (L2) (P2)  27. Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi. (L2) (P2)  28. Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. (L2) (P2)  29. Tīkla aizsardzības rīki: maršrutētāja konfigurācijas optimizācija, ugunsmūri, VPN tīkli. (P2)  30. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija. (L2)  31. Mākoņpakalpojumu un tīkla datu glabātuvju drošība gan no tehnisko gan no juridisko aspektu viedokļa. (L4)  *L - lekcija*  *S - seminārs*  *P - praktiskie darbi* | |
| Studiju rezultāti | |
| Zināšanas:  1. Pārzin kiberdrošības pamatus, drošību internetā un digitālo ierīču un tīkla kiberhigiēnu.  2. Pārzin tīkla etiķeti (netiķeti), digitālo saziņas līdzekļu izmantošanas kultūru.  3. Pārzin personas datu apstrādes tiesiskuma aspektus, Latvijas un Eiropas regulējumu personas datu apstrādes jomā.  4. Pārzin dažādus uzbrukumu veids, tai skaita sociālas inženierijas pamatus.  5. Pārzin informācijas sistēmu, operētājsistēmu drošības pārvaldības labas prakses principus.  6. Pārzin kriptografijas pamatus un internetā pielietotās informācijas šifrēšanas tehnoloģijas.  7. Pārzin datortīkla drošības pamatus: drošības savienojuma izveide, droša lietotāju autentifikācija (t.sk. divfaktoru autentifikācija).  8. Pārzin videonovērošanas un telpu piekļuves kontroles sistēmu īpatnības, uzstādīšanas un uzturēšanas pamatprincipus.  Prasmes:  9. Prot pielietot zināšanas par kiberdrošības un personas datu aizsardzības aspektiem ikdienas dzīvē.  10. Prot identificēt veidus, kā aizsargāt personas datus no trešajam personām, t.sk. izmantojot digitālas drošības tehnoloģijas.  11. Prot veikt informācijas sistēmu drošības auditu un sistēmas drošības risku analīzi.  12. Prot identificēt CSRF, XSS, DoS, DDos uzbrukumus, SQL injekcijas, kā arī zina ka aizsargāt IKT sistēmas no tiem.  13. Prot veikt organizācijās darbinieku apmācības par kiberdrošības pamatiem un ikdienas kiberhigienas nepieciešamību.  14. Prot veikt datu un sistēmu šifrēšanu, lai nodrošināt informācijas konfidencialitāti.  Kompetences:  15. Iekļaujas diskusijās par personu un uzņēmumu informatīvo drošību, kiberdrošību.  16. Prot atpazīt digitālās transformācijas darbā. | |
| Studējošo patstāvīgo darbu organizācijas un uzdevumu raksturojums | |
| Studējošo patstāvīgais darbs – 144 akad. st.: Studējošie patstāvīgi gatavojas nodarbībām, lasot un analizējot docētāja piedāvātos materiālus, analizējot nepieciešamo informāciju, kā arī analizējot ierīču, programmnodrošinājuma un sistēmu iespējas (skat. Obligāti izmantojamo un papildus izmantojamo informācijas avotu sarakstu), lasa docētāja papildus piedāvāto literatūru, pilda docētāja sagatavotos uzdevumus. | |
| Prasības kredītpunktu iegūšanai | |
| Studiju kursa apguve tā noslēgumā tiek vērtēta 10 ballu skalā saskaņā ar Latvijas Republikas  normatīvajiem aktiem un atbilstoši "Nolikumam par studijām Daugavpils Universitātē" (apstiprināts DU Senāta sēdē 17.12.2018.,  protokols Nr. 15), vadoties pēc šādiem kritērijiem: iegūto zināšanu apjoms un kvalitāte, iegūtās prasmes un kompetence atbilstoši plānotajiem studiju rezultātiem.  Nodarbību apmeklējums vismaz 60% no kopējā nodarbību skaita (100%)  Noslēguma pārbaudījums – Diferencētā ieskaite, kura tiek īstenotā testa veida.  Tests satur 30-40 jautājumu ar vairākiem atbildes variantiem.  STUDIJU REZULTĀTU VĒRTĒŠANA   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Pārbaudījumu veidi | Studiju rezultāti | | | | | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | 1. Darbs auditorijā, praktisko uzdevumu izpilde | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | | 2. Patstāvīgais darbs | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | | 3. Noslēguma pārbaudījums - Tests | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | | |
| Kursa saturs | |
| Kursa struktūra: lekcijas – 64 st., seminārs - 16 st. praktiskie darbi - 16 st.  Lekciju tēmas:  1. IKT drošības pamatprincipi, kiberdrošība. (L2)  2. Iekšējie datu apstrādes aizsardzības noteikumi. (L2)  3. Vispārīgā datu aizsardzības regula. (L4)  4. Personas datu aizsardzības jēdziens, personas datu apstrādes principi un mērķi. (L4)  5. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība. (L4)  6. Personas datu aizsardzības speciālista funkcijas un pienākumi. (L2)  7. Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums. (L2)  8. Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. (L4)  9. CSRF, XSS uzbrukumi, SQL injekcijas. (L4)  10. Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. (L4)  11. Videonovērošanas un telpu piekļuves kontroles sistēmas. (L4)  12. Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti. (L4)  13. Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati. (L4)  14. Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. (L2)  15. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes. (L4)  16. Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. (L2)  17. Interneta protokolu drošība, TCP, DNS un maršrutēšana. (L2)  18. Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi. (L2)  19. Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. (L2)  20. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija. (L2)  21. Mākoņpakalpojumu un tīkla datu glabātuvju drošība gan no tehnisko gan no juridisko aspektu viedokļa. (L4)  Semināru tēmas:  1. Netiķete. (S2)  2. Informācija, kā tiesiskās aizsardzības objekts. (S2)  3. Kriminālatbildība un administratīvie pārkāpumi informatīvās drošības jomā. (S2)  4. Drošības pasākumu plānošana, risku analīze. (S2)  5. Nesankcionēta piekļuve informācijai, sociālā inženierija, konfidencialitāte. (S4)  6. Personu un uzņēmumu īpašuma apdraudējuma veidi tīklā. (S2)  7. Kiberdrošība gan darbā gan mājas. (S2)  Praktisko darbu tēmas:  1. Sociālā inženierija, netieši un rupja spēka uzbrukumi (CSRF, XSS uzbrukumi un SQL injekcijas). (P2)  2. Videonovērošanas un telpu piekļuves kontroles sistēmas. (P2)  3. Informācijas sistēmu drošības audits. (P2)  4. Tīkla aizsardzības rīki: maršrutētāja konfigurācijas optimizācija, ugunsmūri, VPN tīkli. (P2)  5. Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. (P2)  6. Interneta protokolu drošība, TCP, DNS un maršrutēšana. (P2)  7. Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi. (P2)  8. Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. (P2)  *L - lekcija*  *S - seminārs*  *P - praktiskie darbi* | |
| Obligāti izmantojamie informācijas avoti | |
| Normatīvie akti:  1. Elektronisko dokumentu likums.  2. Fizisko personu datu apstrādes likums (FPDAL).  3. Vispārīgā datu aizsardzības regula (VPDAR).  4. Valsts informācijas sistēmu likums.  5. Informācijas atklātības likums.  6. Informācijas sabiedrības pakalpojumu likums.  7. Informācijas tehnoloģiju drošības likums.  8. Nacionālās drošības koncepcija.  9. Nacionālās drošības likums.  10. Latvijas kiberdrošības stratēģija.  11. Ministru kabineta noteikumi Nr.442  "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".  12. Ministru kabineta noteikumi Nr.100  „Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība”.  13. Ministru kabineta noteikumi Nr.327  „Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam”.  14. Elektronisko sakaru likums.  15. Informācijas tehnoloģiju un drošības risku pārvaldības normatīvie noteikumi  16. Eiropas Parlamenta un Padomes direktīva COM(2010) Par uzbrukumiem informācijas sistēmām.  17. Latvijas Republikas Nacionālās drošības koncepcija. “Par Nacionālās drošības koncepcijas apstiprināšanu”.  Vadlīnijas un informatīvi materiāli:  1. Informācijas sistēmu drošības pārbaudes vadlīnijas (VARAM).  2. Personas datu apstrādes sistēmu audita rokasgrāmata. –  http://www.dvi.gov.lv/fpda/files/fpda\_audita\_rokasgramata.pdf  E-Gramatas:  ~~1. Ross J. Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, 2008, https://terrorgum.com/tfox/books/security\_engineering \_a\_guide\_to\_building\_dependable\_distributed\_systems.pdf~~  2. Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone “Computer Security Incident Handling Guide” http://dx.doi.org/10.6028/NIST.SP.800-61r2  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf  3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems, http://www.itref.ir/uploads/editor/2ef522.pdf  un plānošana; Aizsardzības līdzekļu izvēle; Tīklu drošības pārvaldīšanas ieteikumi.»  ~~4. Uldis Miķelsons, Informācijas sistēmu drošība: http://www.eksperts.gold.lv/Informacijas\_sistemu\_drosiba.pdf~~  Elektroniskie resursi:  ~~1. “Vēstuļu rakstīšanas VADLĪNIJAS”, Valsts kanceleja, 2017.gads~~ [~~https://www.mk.gov.lv/sites/mk/files/media\_file/vestulu\_vadlinijas\_2017.pdf~~](https://www.mk.gov.lv/sites/mk/files/media_file/vestulu_vadlinijas_2017.pdf)  2. Latvijas Drošāka interneta centrs – Sadaļa “Materiāli” (materiālu bibliotēkā)  <https://drossinternets.lv/lv/materials>  3. Latvijas Republikas droša elektroniska paraksta nodrošinātājā mājaslapa  <https://www.eparaksts.lv/>  4. Latvijas Republikas pārvaldes pakalpojumu portāls  <https://latvija.lv/> un Tehniskās palīdzības materiāli: <https://latvija.lv/lv/ParPortalu/Teh-materiali>  5. Portāls, kurā integrēti vairāki e-pakalpojumi, kuri apkopo datus no Latvijas pašvaldībām, valsts iestādēm un komercsabiedrībām  <https://www.epakalpojumi.lv/>  Esidross.lv - vietne, kurā apkopota noderīga informācija tiem, kam rūp sava un sava datora, telefona vai citu viedierīču drošība internetā.:  6. Sadaļa “Dati un privātums” <https://www.esidross.lv/kategorijas/dati-un-privatums/>  7. Sadaļa “Iekārtas un programmas” <https://www.esidross.lv/kategorijas/iekartas-un-programmas/>  8. Sadaļa “Sociālie tīkli” <https://www.esidross.lv/kategorijas/socialie-tikli/>  9. Sadaļa “Kiberdrošība darbavietā” <https://www.esidross.lv/kategorijas/parolize/>  CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija) struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā IT drošības likuma ietvaros.:  10. Sadaļa “Noderīgi materiāli” <https://cert.lv/lv/par-mums/noderigi-materiali>  11. Informācijas sistēmu drošības riska pārvaldība: politika darbiniekiem https://www.atea.com/media/2ppev0vq/atea-information-security-aug2019\_lv.pdf | |
| Papildus informācijas avoti | |
| Elektroniskie resursi:  1. “Vēstuļu rakstīšanas VADLĪNIJAS”, Valsts kanceleja, 2017.gads https://www.mk.gov.lv/sites/mk/files/media\_file/vestulu\_vadlinijas\_2017.pdf  Literatūrā:  1. ”E-pakalpojumi Latvijā Preces un pakalpojumi internetā”, 2015.gads,  <https://www.zrkac.lv/dev_webadm/doc/e_scouts/e_pakalpojumi_eScouts_final.pdf>  2. Ross J. Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, 2008, https://terrorgum.com/tfox/books/security\_engineering \_a\_guide\_to\_building\_dependable\_distributed\_systems.pdf  3. Uldis Miķelsons, Informācijas sistēmu drošība: http://www.eksperts.gold.lv/Informacijas\_sistemu\_drosiba.pdf  Tiešsaistes uzdevumi:  <https://www.uzdevumi.lv/p/datorika>  Sadaļas:  1. Tīmekļa pārlūkprogramma, informācijas meklēšana  2. Drošība un internets  3. E-pakalpojumi  4. Datu organizācija  5. Tekstapstrāde  6. Prezentācijas un mākoņpakalpojumi | |
| Periodika un citi informācijas avoti | |
| Interneta avoti: 1. Latvijas Drošāka interneta centrs – Sadaļa “Jaunumi”  <https://drossinternets.lv/lv/posts>  2. Esidross.lv - vietne, kurā apkopota noderīga informācija tiem, kam rūp sava un sava datora, telefona vai citu viedierīču drošība internetā. – Sadaļa “Aktivitātes”  <https://www.esidross.lv/kategorijas/aktivitates/>  3. CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija) struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā IT drošības likuma ietvaros. – Sadaļa “Ziņas” <https://cert.lv/lv/zinas>  4. <https://mana.latvija.lv/> | |
| Piezīmes | |
| Kurs tiek docēts latviešu valodā | |