**DAUGAVPILS UNIVERSITĀTES**

**STUDIJU KURSA APRAKSTS**

|  |  |
| --- | --- |
| Studiju kursa nosaukums | **Kiberdrošības pamati un sistēmu aizsardzība pret kiberuzbrukumiem** |
| Studiju kursa kods (DUIS) | DatZP027 |
| Zinātnes nozare | Datorzinātne |
| Kursa līmenis |  |
| Kredītpunkti | 6 |
| ECTS kredītpunkti | 9 |
| Kopējais kontaktstundu skaits | 240 |
| 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. Andris Vagalis, Mg.sc.comp., lekt. Andrejs Radionovs | |
| Priekšzināšanas | |
| Nav nepieciešamas | |
| 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. Netiķete. Kiberdrošība gan darbā gan mājas. (L2) (S4) 2. Iekšējie datu apstrādes aizsardzības noteikumi. Informācija, kā tiesiskās aizsardzības objekts. (L2) (S2) 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. Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums. Kriminālatbildība un administratīvie pārkāpumi informatīvās drošības jomā. (L4) (S2) 7. Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. Nesankcionēta piekļuve informācijai, sociālā inženierija, konfidencialitāte. (L4) (S4) 8. CSRF, XSS uzbrukumi, SQL injekcijas. Sociālā inženierija, netieši un rupja spēka uzbrukumi (CSRF, XSS uzbrukumi un SQL injekcijas). (L4) (P2) 9. Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. (L4) 10. Videonovērošanas un telpu piekļuves kontroles sistēmas. (L4) (P2) 11. Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti. Drošības pasākumu plānošana, risku analīze. (L4) (S2) 12. Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati. Informācijas sistēmu drošības audits. (L4) (P2) 13. Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. Personu un uzņēmumu īpašuma apdraudējuma veidi tīklā. (L2) (S2) 14. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes. (L4) 15. Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. (L2, P2) 16. Interneta protokolu drošība, TCP, DNS un maršrutēšana. (L2, P2) 17. Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi. (L2, P2) 18. Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. (L2, P2) 19. Tīkla aizsardzības rīki: maršrutētāja konfigurācijas optimizācija, ugunsmūri, VPN tīkli. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija. (P2) (L2) 20. 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. Zina kiberdrošības pamatus, drošību internetā un digitālo ierīču un tīkla kiberhigiēnu. 2. Zina tīkla etiķeti (netiķeti), digitālo saziņas līdzekļu izmantošanas kultūru. 3. Zina par personas datu apstrādes tiesiskuma aspektus, Latvijas un Eiropas regulējumu personas datu apstrādes jomā. 4. Zina dažādus uzbrukumu veidus, tai skaita sociālas inženierijas pamatus. 5. Zina par informācijas sistēmu, operētājsistēmu drošības pārvaldības labas prakses principus. 6. Zina kriptografijas pamatus un internetā pielietotās informācijas šifrēšanas tehnoloģijas. 7. Zina datortīkla drošības pamatus: drošības savienojuma izveide, droša lietotāju autentifikācija (t.sk. divfaktoru autentifikācija). 8. Zina videonovērošanas un telpu piekļuves kontroles sistēmu īpatnības, uzstādīšanas un uzturēšanas pamatprincipus.   PRASMES:   1. Prot pielietot zināšanas par kiberdrošības un personas datu aizsardzības aspektiem ikdienas dzīvē. 2. Prot identificēt veidus, kā aizsargāt personas datus no trešajam personām, t.sk. izmantojot digitālas drošības tehnoloģijas. 3. Prot veikt informācijas sistēmu drošības auditu un sistēmas drošības risku analīzi. 4. Prot identificēt CSRF, XSS, DoS, DDos uzbrukumus, SQL injekcijas, kā arī zina ka aizsargāt IKT sistēmas no tiem. 5. Prot veikt organizācijās darbinieku apmācības par kiberdrošības pamatiem un ikdienas kiberhigienas nepieciešamību. 6. Prot veikt datu un sistēmu šifrēšanu, lai nodrošināt informācijas konfidencialitāti.   KOMPETENCE:   1. Spēj iekļauties diskusijās par personu un uzņēmumu informatīvo drošību, kiberdrošību. 2. Spēj atpazīt digitālās transformācijas darbā. | |
| Studējošo patstāvīgo darbu organizācijas un uzdevumu raksturojums | |
| Patstāvīgā darba organizācija un uzdevumi: Referāta un prezentācijas sagatavošana par studiju kursā iekļautajiem normatīvajiem aktiem un informācijas sistēmu izpēti. | |
| 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.  Priekšnosacījumi pārbaudījuma kārtošanai: Pozitīvi jāaizstāv prezentācija, praktiskais darbs informācijas ievadē un meklēšanā, praktiskajās nodarbībās jāveic docētāja uzdotie uzdevumi. Sekmju kontroles forma: Praktisks eksāmens, kas sastāv no testa un praktiskā uzdevuma.  STUDIJU REZULTĀTU VĒRTĒŠANA   |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Pārbaudījumu veidi | Studiju rezultāti | | | | | | | | | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | | Patstāvīgais darbs | + | + | + | + | + | + | + | + | | Praktiskais darbs | + | + | + | + | + | + | + | + | | Eksāmens | + | + | + | + | + | + | + | + | | |
| Kursa saturs | |
| Kursa struktūra: lekcijas – 64 st., seminārs – 16 st. praktiskie darbi – 16 st.  Lekciju tēmas:   1. IKT drošības pamatprincipi, kiberdrošība. Iekšējie datu apstrādes aizsardzības noteikumi. (L4) 2. Vispārīgā datu aizsardzības regula. (L4) 3. Personas datu aizsardzības jēdziens, personas datu apstrādes principi un mērķi. (L4) 4. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība. (L4) 5. Personas datu aizsardzības speciālista funkcijas un pienākumi. (L2) 6. Atbildība par pārkāpumiem personas datu aizsardzības jomā, informācijas atklātības likums. (L2) 7. Uzbrukumu veidu apskats. Sociālā inženierija, netieši un rupja spēka uzbrukumi. (L4) 8. CSRF, XSS uzbrukumi, SQL injekcijas. (L4) 9. Aparatūras un fiziskā drošība – uzbrukumi un aizsardzības veidi. (L4) 10. Videonovērošanas un telpu piekļuves kontroles sistēmas. (L4) 11. Informācijas drošības pamatprincipi, risku analīze, drošības pārvaldība, tehniskie līdzekļi, drošības incidenti. (L4) 12. Informācijas sistēmu drošības pārvaldība organizācijās, par IS drošību atbildīgie darbinieki un organizācijās darbinieku apmācības stratēģija. IS drošības audita pamati. (L4) 13. Tīklu un kritiskās infrastruktūras uzbūve tās komponentes. (L2) 14. Kritiskās infrastruktūras tīklu savstarpējā atkarība, drošības riski un aizsardzības metodes. (L4) 15. Mazāko privilēģiju princips, piekļuves vadība un operētājsistēmu drošība. (L2) 16. Interneta protokolu drošība, TCP, DNS un maršrutēšana. (L2) 17. Nevajadzīgās datu plūsmas: servisa atteikumu uzbrukuma veidi. DoS un DDoS uzbrukumi. (L2) 18. Kriptogrāfija. Šifrēšanas protokols SSL/TLS. HTTPS. (L2) 19. Tīmekļa drošības modelis, sesiju vadība un lietotāju autentifikācija. (L2) 20. 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) | |
| Obligāti izmantojamie informācijas avoti | |
| 1. Borzovs, J., Ziemele, I. Informācijas sabiedrības tiesību pamati. Rīga: Rīgas Stradiņa universitāte, 2022, 679 lpp. 2. Digitalizācija un sabiedrība. Rakstu krājums. Zinātniskā redaktore Anda Rožukalne. Jelgava: Jelgavas tipogrāfija, 2021, 143 lpp. 3. Miķelsons, M. Informācijas sistēmu drošība. 2011. Pieejams: http://www.eksperts.gold.lv/Informacijas\_sistemu\_drosiba.pdf | |
| Papildus informācijas avoti | |
| 1. Par Latvijas kiberdrošības stratēģiju 2023.–2026. gadam. Ministru kabineta rīkojums Nr. 158, Rīgā: 2023. 2. Biometrijas datu apstrādes sistēmas likums. 3. Elektronisko dokumentu likums. 4. Fizisko personu datu aizsardzības likums. 5. Informācijas atklātības likums. 6. Sodu reģistra likums. 7. Valsts informācijas sistēmu likums. 8. Par Konvenciju par kibernoziegumiem un Konvencijas par kibernoziegumiem Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās. 9. LR IeM noteikumi nr. 20 „Noteikumi par datortehnikas un datortīklu lietošanas kārtību Iekšlietu ministrijā un tās padotībā esošajās iestādēs” (2006.05.24.) 10. MK 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”. 11. Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone “Computer Security Incident Handling Guide” https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf 12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems, http://www.itref.ir/uploads/editor/2ef522.pdf 13. Šmite, D., Dosbergs, D., Borzovs, J. Informācijas un komunikācijas tehnoloģijas nozares tiesību standartu pamati. Rīga: LU Akadēmiskais apgāds, 2005, 208 lpp. 14. Vēža V. red. Datortīkli un interneta pakalpojumu izmantošana. Datorzinību pamati. Rīga, LU: Mācību grāmata, 2000. | |
| Periodika un citi informācijas 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. Portāla Latvija.lv atbalsta vietne: https://mana.latvija.lv/ | |
| Piezīmes | |
| Īsā cikla profesionālās augstākās izglītības studiju programmas „Civilā drošība un aizsardzība” studiju kurss.  Kurss tiek docēts latviešu valodā. | |