RTU studiju kurss "Ievads informācijas sistēmu drošībā"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE1020
Nosaukums	Ievads informācijas sistēmu drošībā
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles; Brīvās izvēles
Atbildīgais mācībspēks	Imants Gorbāns - Doktors, Docents
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kursā tiek aplūkoti informācijas sistēmu drošības jēdzieni, pamatprincipi, apdraudējumu veidi un speciāli risinājumi informācijas sistēmu drošības uzlabošanai. Tiek aplūkoti starptautiskie un Latvijas normatīvie akti un standarti IT drošības jomā, kā arī drošības līdzekļu tehnoloģiskie risinājumi. Studiju kursā aplūkotie IT drošības pamatprincipi noderēs IT konsultanta darbā, kā arī sistēmu projektēšanā, uzturēšanā, uzlabošanā un drošības incidentu analīzē.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir sniegt zināšanas informācijas sistēmu drošībā, kiberdrošībā; sagatavot speciālistus ar kompetencēm informācijas sistēmu drošības analīzē un drošības risku vadībā. Studiju kursa galvenie uzdevumi: - attīstīt prasmes identificēt informācijas sistēmu reālās problēmas, analizēt to sarežģītību un novērtēt risinājumu variantus; - iemācīt identificēt IT drošības riskus un izvēlēties piemērotus drošības līdzekļus risku mazināšanai, sekot jaunākajai nozares informācijai.
Patstāvīgais darbs, tā organizācija un uzdevumi	Pēc lekcijas studentiem ir jāizpilda īss tests par lekcijas tēmu. Semestra laikā studentiem mājās jāizpilda un jāiesniedz ORTUS e-studiju vidē divi praktiskie darbi un kursa nobeiguma darbs. Šie darbi ir jāaizstāv semināros vai konsultācijās.

Literatūra	Obligātā/Obligatory: 1. Jean Andrews, Joy Dark, Jill West. CompTIA A+ Core 2 Exam Guide to Operating Systems and Security. Cengage, USA, 2020, ISBN: 978-0-357-10850-5. 2. John R. Vacca. Computer and Information Security Handbook. Elsevier, 2017, ISBN 978-0-12-803843-7 - https://books.google.lv/books?id=05HUDQAAQBAJ&lpg=PP1&hl=lv&pg=PP1#v=onepage&q&f=false (13.10.2024). 3. Don Franke. Cyber Security Basics: Protect your organization by applying the fundamentals. CreateSpace Independent Publishing Platform, 2016. 101 pp. 4. John Uwaya. Fundamental Cyber, Computing and Telephone Security. CreateSpace Independent Publishing Platform, 2018. 104 pp. 5. GDPR and Cyber Security for Business Information Systems; River Publishers (2018); ISBN: 8793609132. 6. Science of Cyber-Security. JASON, The MITRE Corporation - http://www.fas.org/irp/agency/dod/jason/cyber.pdf (13.10.2024). Papildu/Additional: 1. Designing an Authentication System: a Dialogue in Four Scenes - https://web.mit.edu/kerberos/dialogue.html (13.10.2024). 2. Kerberos – https://web.mit.edu/kerberos/, https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview (13.10.2024). 3. Attacking Network Protocols; No Starch Press; 1 edition (2017); ISBN: 1593277504 (13.10.2024). 4. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide (Isc Official Study Guides; Sybex; 8th edition (2018); ISBN: 1119475937. 5. Wenliang Du. Computer Security: A Hands-on Approach. 2019, ISBN 1733003908, 9781733003902. 6. CERT IT drošības normatīvie akti - https://cert.lv/lv/normativie-akti-un-it-drosibas-politika (13.10.2024). 7. Latvijas Bankas Finanšu tehnoloģiju uzraudzības pārvaldes rekomendētais kontrolsaraksts informācijas tehnoloģiju un drošības pārvaldības pašvērtējumam – https://datnes.latvijasbanka.lv/tiesibu-akti/Skaidrojumi/kontrolsaraksts_IT_drosibas_parvaldibas_pasvertejumam.pdf (13.10.2024). Citi informācijas avoti/ Other sources of information: 1. Valsts informācijas sistēmu likums - https://likumi.lv/ta/id/62324-valsts-informacijas-sistemu-likums (13.10.2024). 2. Nacionālās kiberdrošības likums - https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums (13.10.2024). 3. Eiropas Parlamenta un Padomes regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 – https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32022R2554 (13.10.2024). 4. Eiropas Parlamenta un Padomes direktīva par uzbrukumiem informācijas sistēmām. 2013/40/ES - https://eur-lex.europa.eu/eli/dir/2013/40/oj (13.10.2024). 5. Eiropas Parlamenta un Padomes NIS2 direktīva (angļu v.) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN (02.01.2025). 6. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula) 2016/679 - http://data.europa.eu/eli/reg/2016/679/oj (13.10.2024). 7. Cyber security design principles - https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles (20.10.2024) 8. IEEE Publications – https://www.ieee.org/publications/index.html (to search).
Nepieciešamās priekšzināšanas	Operētājsistēmu prasmīgas lietošanas un konfigurēšanas pamati.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
1. IT drošības aptvērums. Kibernoziedzība, kiberkarš, IT iespēju radītie riski, ievainojamības, apdraudējumi. Populārākie uzbrukumu veidi (vīrusi, tārpi, koda ekspluatējumi, ļaunatūra u. c.).	2	2	0	0
2. Pamata jēdzieni. Autentifikācija, autorizācija, žurnalēšana; konfidencialitāte, veselums, pieejamība. Resursi un drošības līdzekļu tipi (preventīvie, atklājošie, labojošie). Risku analīzes un risku mazināšanas jēdzieni. Nozares jaunumi.	2	2	0	0
3. Normatīvie akti un standarti. Starptautiskie regulējumi (ISO sērija 27, Vispārīgā datu aizsardzības regula, ES normatīvie akti), Latvijas likumi un noteikumi par IT drošības jomu; atsevišķu nozaru, piemēram, finanšu institūciju īpašie regulējumi.	2	2	0	0
4. Svarīgākie drošības līdzekļi datu un citu resursu aizsardzībai. ISO 27002 standarts par drošības līdzekļiem. Noslēpums, publiskās un privātās atslēgas, asimetriskā šifrēšana, Kerkhofa princips, Šanona maksima, šifru veidi, brutāla spēka uzbrukums, jaucējfunkcijas kolīzijas. Šifrēšanas algoritmi, standarti, protokoli, elektronisko parakstu algoritmi.	6	6	0	0
5. Resursi, to ievainojamības un drošības līdzekļi risku mazināšanai. Identitātes vadība un piekļuves kontrole, rezerves kopijas, žurnālfaili. Datoru specifikācijas datu drošībai, datu centru fiziskā aizsardzība. Daudzfaktoru autentifikācija. Uz laiku un skaitītāju balstīti žetoni, sertifikāti.	4	4	0	0
6. Autentifikāciju un autorizāciju protokoli. Kerberos protokols. Bezvadu savienojumu drošība. Mobilās ierīces organizācijā.	4	4	0	0
8. Drošības pārvaldība organizācijā. Administratīvās un tehniskās politikas, lomas, privilēģiju piešķiršana. Pienākumu atdalīšana.	2	2	0	0
7. Ievads datortīklu drošībā (žurnālfailu analīze, tīkla sadalīšana, ugunsmūri, starpniekserveri, tīmekļa servisi, virtuālās mašīnas u. c.). Datortīkla drošības pastiprināšana. Tīkla notikumu uzraudzība un analīze.	2	2	0	0
9. IT risinājumu izstrādes un programmatūras drošība. Ievads drošības testēšanā: ievainojamību skenēšana, ielaušanās testi, sociālās inženierijas testi, programmatūras testēšana izstrādes procesā.	2	2	0	0

10. Drošas sistēmu arhitektūras. Drošība mikroservisu arhitektūras risinājumos un mākoņskaitļošanas vidē.	2	2	0	0
11. Lietu internets un tā drošība. Nākotnes vīzijas IT risku un drošības jautājumos, IT tehnoloģiju izmantošanas riski visdažādākajās cilvēku darbības jomās. Labās prakses piemēri.	2	2	0	0
Semināri un praktiskie darbi par drošības līdzekļiem.	4	4	0	0
Kursa nobeiguma darbs. Seminārs, nobeiguma darbu aizstāvēšanai un apspriešanai.	2	2	0	0
Eksāmens.	4	4	0	0
Kopā:	40	40	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Prot lietot un integrēt zināšanas un izpratni par informācijas sistēmu drošību ar citu datorzinātņu disciplīnām savas specializācijas jomas studiju un profesionālās darbības atbalstam.	Testi, kursa nobeiguma darbs, eksāmens. Kritēriji: izprot IT drošības aptvērumu, pamata jēdzienus; sekmīga vērtējuma saņemšanai jāizpilda vairāk nekā 50 % no darba apjoma
Prot identificēt IT drošības riskus, identificēt produkcijas un izstrādes vides problēmas, analizēt to sarežģītību un novērtēt iespējas tās risināt. Orientējas normatīvajos aktos.	Praktiskais darbs Nr. 1 par datu drošību, normatīvajiem aktiem un šifrēšanu; darbs jāiesniedz e-studiju vidē un jāaizstāv seminārā, testi, eksāmens. Kritēriji: spēj pielietot starptautiskos un Latvijas normatīvos aktus IT drošības problēmu risināšanā.
Spēj lietot datortīklu novērošanas, vadības un aizsardzības līdzekļus, konfigurēt datoru un mobilo ierīču operētājsistēmas to drošības uzlabošanai un drošai saziņai. Prot izvēlēties piemērotas autentifikācijas metodes, izveidot drošus saziņas kanālus, šifrēt datus.	Praktiskais darbs Nr. 2 par autentifikāciju un autorizāciju mehānismiem, datortīkla novērošanu; darbs jāiesniedz e-studiju vidē un jāaizstāv seminārā, testi, nobeiguma darbs, eksāmens. Kritēriji: spēj analizēt tīkla notikumus, izvēlēties atbilstošus risinājumus.
Spēj argumentēti un terminoloģiski pareizi diskutēt par kiberdrošības risinājumu izvēli uzņēmuma problēmu risināšanā. Spēj konsultēt lietotājus, IT speciālistus un organizācijas vadību IT drošības jautājumos.	Semināri, kursa nobeiguma darbs, eksāmens. Kritēriji: spēj prezentēt kompleksu IT drošības redzējumu.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Praktiskais darbs Nr. 1	20
Praktiskais darbs Nr. 2	10
Kursa nobeiguma darbs	30
Testi pēc lekcijām	10
Eksāmens	30
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi			Brīvās izvēles pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs	Ieskaite	Eksām.	Darbs
1.	3.0	28.0	12.0	0.0		*				