RTU studiju kurss "Informatīvo sistēmu drošība"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0566
Nosaukums	Informatīvo sistēmu drošība
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles; Brīvās izvēles
Atbildīgais mācībspēks	Imants Gorbāns - Doktors, Docents
Mācībspēks	Vadims Žuravļovs - Doktors, Docētājs Normunds Kante - Pētnieks
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kursā tiek aplūkoti informācijas sistēmu drošības pamatprincipi, apdraudējumu veidi un speciāli risinājumi informācijas tehnoloģiju (IT) drošības uzlabošanai. Ir aplūkotas autentifikācijas metodes, autorizācija, šifrētu savienojumu izveide ar dažādām atslēgām, Kerberos, SSL, TLS, VPN, OAuth u.c. Studiju kursā aplūkotie IT drošības principi noderēs sistēmu projektēšanā, uzturēšanā, uzlabošanā, notikumu analīzē.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir sniegt fundamentālas un lietišķas zināšanas informācijas sistēmu drošībā, kiberdrošībā, informātikas inženierijā; sagatavot speciālistus ar kompetencēm informācijas sistēmu drošības analīzē, sistēmu projektēšanā, uzturēšanā, drošības risku vadībā. Studiju kursa uzdevumi: - veidot kompetences identificēt reālās IT vides problēmas; - attīstīt studējošo prasmes analizēt to sarežģītību un novērtēt to risināšanas optimālākos variantus; - uzlabot studējošo prasmes identificēt IT drošības riskus; - attīstīt studējošo prasmes lietot datortīklu vadības un aizsardzības līdzekļus.
Patstāvīgais darbs, tā organizācija un uzdevumi	Lekcijas laikā mācībspēks prezentē studējošiem teorētisko materiālu un praktiskās realizācijas piemērus. Katras lekcijas beigās studentiem ir jāizpilda īss tests ar dotās lekcijas tēmu. Semestra laikā studentiem ir 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. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide (Isc Official Study Guides; Sybex; 8th edition (2018); ISBN: 1119475937. 2. GDPR and Cyber Security for Business Information Systems; River Publishers (2018); ISBN: 8793609132. 3. Attacking Network Protocols; No Starch Press; 1 edition (2017); ISBN: 1593277504. 4. Science of Cyber-Security. JASON, The MITRE Corporation - http://www.fas.org/irp/agency/dod/jason/cyber.pdf. 5. Designing an Authentication System: a Dialogue in Four Scenes - https://web.mit.edu/kerberos/dialogue.html. 6. Wenliang Du. Computer Security: A Hands-on Approach. 2019, ISBN 1733003908, 9781733003902. 7. James Graham, Ryan Olson, Rick Howard. Cyber Security Essentials. CRC Press, 2016 ISBN 1439851263, 9781439851265. 8. John R. Vacca. Computer and Information Security Handbook. Elsevier, 2017, ISBN 978-0-12-803843-7. Papildu/Additional: 1. IEEE - https://www.ieee.org/ 2. CERT - https://cert.lv/lv/ 3. Kerberos - https://web.mit.edu/kerberos/ 4. Valsts informācijas sistēmu likums. Pieņemts: 02.05.2002. 5. Elektronisko sakaru likums. Pieņemts: 28.10.2004. 6. Eiropas Parlamenta un Padomes direktīva par uzbrukumiem informācijas sistēmām. 2013/40/ES 7. 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.
Nepieciešamās priekšzināšanas	Prasmīga lietotāja kompetences darbā ar datoru.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Ievads IT drošībā: autentifikācija, autorizācija, uzskaite, konfidencialitāte, veselums, pieejamība, ievainojamības, riski, apdraudējumi, vīrusi, tārpi, koda ekspluatējumi, hakeri, ļaunatūra.	2	2	0	0
Reklāmas, trojāni, izspiedējvīrusi, robottīkli, backdoor, rootkit, loģiskās bumbas, viltus Wi-Fi AP, DNS kešatmiņas saindēšana, DoS, DDoS, XSS, uzbrukumi parolēm, sociālā inženierija.	2	2	0	0
Šifrēšanas algoritmi, noslēpums, publiskas un privātas atslēgas, vēsturiskie šifri, Kerkhofa princips, Šanona maksima, kriptoloģija, šifru veidi, brutāla spēka uzbrukums. RC4, TLS ar AES GCM.	2	2	0	0

Asimetriskas kriptosistēmas, publiskās atslēgas. MAC, HMAC, CMAC, CBC-MAC, RSA, DH, PKI, DSA. Digitālo parakstu algoritmi, heša kolīzijas. TLS/ SSH, PGP SSH, IPsec, HTTPS, SSL, VPN.	4	4	0	0
Identitātes vadība un piekļuves kontrole, failu serveri. Datu drošība, TPM 1.2 un TPM 2, BitLocker, Filevault 2, dm-crypt, Secure Boot. Datu aizsardzība Eiropā, GDPR.	2	2	0	0
Praktiskais darbs Nr. 1. Seminārs par autentifikāciju mehānismiem un datu šifrēšanu.	2	2	0	0
Daudzfaktoru autentifikācija: kaut kas, ko jūs zinat; kaut kas, kas jums ir; kaut kas, kas jūs esat. Uz laiku un skaitītāju balstīti žetoni, sertifikāti, CRL, LDAP, TLS.	2	2	0	0
Kerberos autentifikāciju protokoli. OAuth, OpenID. Tīkla drošība, RADIUS, mobilās ierīces organizācijā, bezvadu savienojumi, WPA, TKIP, WPA2, PIN, NFC, 802.1x. Atrašanās vietas izmantošana.	4	4	0	0
Datortīkla stiprināšana, žurnālfaili, notikumu analīze, tīkla sadalīšana, DHCP, ARP, EAP-TLS. Ugunsmūri, starpniekserveri, reversie starpniekserveri, tīmekļa servisi, virtuālās mašīnas, dokeri.	2	2	0	0
Praktiskais darbs Nr. 2. Seminārs par autentifikāciju mehānismiem un datu šifrēšanu.	2	2	0	0
Administratīvās un tehniskās politikas, lomas, privilēģiju piešķiršana.	2	2	0	0
Informācijas sistēmu vadība, riska vadība un biznesa procesu plānošana. Kredītkaršu maksājumu sistēmas. Notikumu uzraudzības un vadības sistēmas, ievainojamību skanēšana un testēšana.	4	4	0	0
Lietu internets, IoT drošība. Nākotnes vīzijas IT risku un drošības jautājumos. Labā prakse.	2	2	0	0
Kursa nobeiguma darbs. Seminārs, nobeiguma darbu aizstāvēšanai un apspriešanai.	4	4	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 pielietot un integrēt zināšanas un izpratni par informācijas sistēmu drošību ar citu datorzinātņu disciplīnām savas specializācijas jomas studiju un darba atbalstam.	Praktiskie darbi, nobeiguma darbs, testi, eksāmens.
Prot identificēt IT drošības riskus, izmantot žurnālfailus, identificēt reālās vides problēmas, analizēt to sarežģītību un novērtēt iespējas tās atrisināt ar informācijas tehnoloģijām.	Praktiskie darbi, nobeiguma darbs, testi, eksāmens.
Spēj lietot datortīklu vadības un aizsardzības līdzekļus, konfigurēt tīklu operētājsistēmas Windows, Linux, MacOS to drošības uzlabošanai un drošai saziņai.	Praktiskie darbi, nobeiguma darbs, testi, eksāmens.
Prot izvēlēties optimālas autentifikācijas metodes, izveidot drošus saziņas kanālus, ģenerēt sertifikātus, šifrēt datus, kā arī sagatavot darba atskaiti.	Praktiskie darbi, nobeiguma darbs, testi, eksāmens.
Spēj konsultēt lietotājus un IT speciālistus IT drošības jautājumos.	Praktiskie darbi, nobeiguma darbs, testi, eksāmens.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Divi mājās izpildāmi praktiskie darbi	30
Lekciju iknedēļas mazie testi	10
Kursa nobeiguma darbs un tā aizstāvēšana	20
Eksāmena 1. daļa – lielais tests	20
Eksāmena mutvārdu daļa	20
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	16.0	0.0	16.0		*		*		