RTU studiju kurss "Kiberdrošība jūras transportā"

0J000 Latvijas Jūras akadēmija

Vispārējā informācija

Kods	LJA070
Nosaukums	Kiberdrošība jūras transportā
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācībspēks	Aleksandrs Gasparjans - Doktors, Profesors
Mācībspēks	Andis Maksimovs - Docētājs
Apjoms daļās un kredītpunktos	1 daļa, 3.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kursa ietvaros studējošie iegūst padziļinātu izpratni par uzbrucēju veidiem un motivāciju, kā arī dažādiem aizsardzības līmeņiem, apgūst prasmes atpazīt kiberuzbrukumu galvenos vaininiekus – uzbrucējus. Studējošie apgūst būtiskas atšķirības starp valsts un privātā sektora aizsardzības stratēģijas prioritātēm, kā arī svarīgākās drošības personāla lomas. Patstāvīgā darba ietvaros studējošiem jāizpēta kiberdrošības incidents jūras transportā, jāsagatavo un jāsniedz publiska prezentācija. Bez tā studējošiem jāizpilda grupas uzdevumu par pašu izvēlētu tēmu – par kuģa vai ostas iestādes kiberdrošības politiku. Studiju kursa nobeigumā studējošiem jāizpilda kiberdrošības izpratnes viktorīna.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Studiju kursa mērķis ir padziļināti iepazīstināt studējošos ar kiberdrošību un tās īpašajiem aspektiem jūras transportā. Studiju kursa uzdevumi: 1. Sniegt studējošiem padziļinātas zināšanas par kiberdrošību, informācijas drošību, drošības pamatprincipiem un lietotāju izpratni. 2. Sniegt padziļinātu izpratni par kiberdrošības riskiem un to samazināšanas iespējām gan uz sauszemes, gan uz kuģa jūras apstākļos.
Patstāvīgais darbs, tā organizācija un uzdevumi	Darba uzdevumi: 1. Izpētīt kiberdrošības incidentu, izveidot prezentāciju, kas atbild uz šiem jautājumiem: kas notika, kad, kam uzbruka, kādas metodes tika izmantotas, kādi bija zaudējumi, ko uzņēmums darīja, lai mazinātu problēmu. 2. Jāaizpilda kiberdrošības novērtējums un mācīšanās tests tiešsaistē (Disa.mil.). 3. Aprakstīt izvēlēto izpētes gadījumu par uzņēmumu, kuģi vai jebkuru ostas infrastruktūras objektu, par kiberdrošības jautājumiem un iespējamo seku mazināšanu atbilstoši studējošā izpratnei un iepriekš apspriestajiem paņēmieniem. Darba organizācija: Saskaņā ar individuālo uzdevumu studējošie patstāvīgi, sadarbībā ar mācībspēku gan praktisko nodarbību laikā, gan arī individuālajās konsultācijās izpilda uzdotos darbus, kas tiek veikti saskaņā ar izstrādātajiem noteikumiem un studējošo ētikas normām. Pieejamas individuālas un grupu konsultācijas gan klātienē, gan MS Teams vidē un izmantojot e-pastu.
Literatūra	Obligātā / Obligatory: 1. NIST Cybersecurity Framework, NIST, 2020. 2. If available, CSX Cybersecurity Fundamentals, ISACA, 2015. Papildu / Additional: 1. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf 2. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf 3. Privacy and Cybersecurity resources by ISACA: - http://www.isaca.org/Knowledge-Center/Research/Pages/Cybersecurity.aspx - http://www.isaca.org/Knowledge-Center/Research/Pages/Privacy.aspx Citi informācijas avoti / Other sources of information: ISO:27001 standard.
Nepieciešamās priekšzināšanas	Informācijas un komunikāciju tehnoloģijas (bakalaura programma).

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Ievads informācijas aizsardzībā, pamata drošības principi, biežākie apdraudējumi. Ļaunatūras veidi, paroļu prasības. Piemēri no reālās dzīves.	5	0	2	3
Īsa iepriekšējās tēmas apskate. Drošības lomas uzņēmumā un valsts pārvaldes sistēmās. Drošības kontroles, informācijas aizsardzības principi. Risku analīzes nepieciešamība. Apdraudējumu un biežāko uzbrukumu veidi.	5	0	2	3
Praktiskais uzdevums – atrast un iegūt datus par veiksmīgu kiberdrošības uzbrukumu pēdējo 15 gadu laikā un prezentācijas izveide, kur paskaidrots kas, kad un kā ieguva kāda uzņēmuma/iestādes vērtības.	5	20	2	23
Studentu atrasto notikumu apskats un prezentācijas, diskusijas. Kiberdrošības politikas, drošības slāņi, kiberdrošības kontroles. Kiberdrošība uz kuģiem un jūrā.	5	14	2	17

Risku novērtēšanas piemērs, gadījuma izpēte.	6	0	2	4
Kiberdrošības galda spēle – "Admins & Networks".	0	14	0	14
Norādītā uzņēmuma drošības novērtēšana un uzlabojumu rekomendācijas. Apkopojuma izveide, noformēšana un prezentācija.	3	0	1	2
Kiberdrošības apzināšanās tests – Disa.mijl. izveidotajā testā.	3	0	1	2
Kopā:	32	48	12	68

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Zināšanas: - spēj parādīt zināšanas un izpratni par informācijas drošības pamatprincipiem, lietotāja paradumiem un attieksmi.	Metodes: grupu darbs, individuālais praktiskais darbs, diskusijas, patstāvīgo darbu izstrādāšana un aizstāvēšana. Kritēriji: - spēja parādīt zināšanas un izpratni par informācijas drošības pamatprincipiem; lietotāja paradumiem un attieksmi.
Prasmes: - spēj atrast, apkopot atbilstošus informācijas avotus par kiberrisku samazināšanu, aizsardzības pasākumiem; - spēj veikt vienkāršotu risku analīzi un atbilstoši reaģēt ar drošību saistītās izaicinošās situācijās.	Metodes: grupu darbs, individuālais praktiskais darbs, diskusijas, patstāvīgo darbu izstrādāšana un aizstāvēšana. Kritēriji: - spēja atrast, apkopot atbilstošus informācijas avotus par kiberrisku samazināšanu, aizsardzības pasākumiem; - spēja veikt vienkāršotu risku analīzi un atbilstoši reaģēt ar drošību saistītās izaicinošās situācijās.
Kompetences: - spēj analizēt, novērtēt informācijas drošības apmācības un sniegt priekšlikumus to pilnveidei.	Metodes: grupu darbs, individuālais praktiskais darbs, diskusijas, patstāvīgo darbu izstrādāšana un aizstāvēšana. Kritēriji: - spēja analizēt, novērtēt informācijas drošības apmācības un sniegt priekšlikumus to pilnveidei.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Individuālais praktiskais darbs	25
Darbs praktiskajās nodarbībās (grupu darbs, diskusijas)	25
Patstāvīgo darbu izstrādāšana un aizstāvēšana	50
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	3.0	1.0	1.0	0.0	*		