

Studiju kursa apraksts

Atvērto avotu un datu analīze

Kursa apraksta statuss: Apstiprināts

Kursa apraksta versija: 8.00

Kursa apraksta apstiprināšanas datums: 02.02.2024 12:30:31

Par studiju kursu

Kursa kods:	JF_438	LKI līmenis:	7. līmenis
ECTS:	3.00	Kredītpunkti:	2.00
Zinātnes nozare:	Vadībzinātne		
Mērķauditorija:	Tiesību zinātne		

Studiju kursa vadītājs

Kursa vadītājs:	Daiga Spila
-----------------	-------------

Studiju kursa īstenotājs

Struktūrvienība:	Sociālo zinātņu fakultāte
Vadītājs:	Karina Palkova
Kontaktinformācija:	Dzirciema iela 16, Rīga, szf@rsu.lv

Studiju kursa plānojums

Pilns laiks						
Daļas nr.	Īstenošanas forma	Skaits	Ilgums (ak.st)	Kontaktstundas	Gala pārbaudījums	ECTS
1	Lekcijas	8	2	16	Eksāmens (Rakstisks)	3.00
	Nodarbības	4	2	8		
	Kopā:			24		
Nepilns laiks						
Daļas nr.	Īstenošanas forma	Skaits	Ilgums (ak.st)	Kontaktstundas	Gala pārbaudījums	ECTS
1	Lekcijas	3	2	6	Eksāmens (Rakstisks)	3.00
	Nodarbības	2	2	4		
	Kopā:			10		

Studiju kursa apraksts

Priekšzināšanas:

Prasmes strādāt ar datoru, interneta pārlūkiem, orientēties sociālajos tīklos, angļu valodas prasmes

Mērķis:

Sniegt studentiem izpratni par atvērto avotu un datu analīzes OSINT (Open Source Intelligence) lietošanas gadījumiem ekonomisko noziegumu atklāšanā un apkarošanā;
Sniegt studentiem nepieciešamās prasmes un iemaņas atvērto avotu pierādījumu meklēšanā un apkopošanā, iepazīstinot studentus ar brīvpieejas rīkiem un informācijas iegūšanas metodēm;
Sniegt studentiem prasmes un iemaņas iegūtās informācijas un pierādījumu analīzē un sintēzē.

Tēmu saraksts

Pilns laiks

Nr.	Tēma	Īstenošanas forma	Skaits (norises vieta)
1.	Ievads OSINT Atvēto avotu un datu analīze jeb OSINT kā informācijas vākšanas, apkopošanas un analīzes pieeja; Gadījumu studijas ilustrējot: • Cilvēku dosjē veidošanu; • Ģeolokāciju; • Notikumu rekonstrukciju; • Interesu konflikta identificēšanu.	Lekcijas	0.5 (datorklase)
2.	Ievads mūsdienu interneta vidē Interneta darbības principi – datu aprites infrastruktūra; Interneta vietņu darbības principi – domēnu, serveru hostēšana; Veblapu indeksācija, deepweb, dark web; SEO – search engine optimization; Sociālie tīkli – uzmanības ekonomika, influenceri Lielo datu ekonomika, mašīnmācīšanās Datu brokeri – Cambridge Analytica, OCEAN, micro targeting	Lekcijas	0.5 (datorklase)
3.	Informācijas pieejamība un privātums internetā Semināra darbs atbilstoši semināra Nr. 1 instrukcijai.	Nodarbības	0.25 (datorklase)
4.	Avancēta meklēšana interneta pārlūkos Interneta pārlūku dorkings: • Meklēt konkrētā lapā; • Meklēt konkrētu frāzi; • Meklēt konkrētu failu tipu; • Meklēt pēc attēla u.c. Arhivētais saturs; Personas datu meklēšana pēc personas vārda, lietotāja vārda, e-pasta, adreses, telefona numura	Lekcijas	0.5 (datorklase)
5.	Meklēšana sociālajos tīklos Facebook; Twitter; Instagram; VKo ntakte; YouTube; WhatsApp grupas; Telegram kanāli un grupas.	Lekcijas	0.5 (datorklase)
6.	Personas dosjē apkopošana Semināra darbs atbilstoši semināra Nr. 2 instrukcijai.	Nodarbības	0.25 (datorklase)
7.	Pierādījumu verificēšana Teksta pārbaude; Attēlu pārbaude; Video pārbaude; Lokācijas pārbaude.	Lekcijas	1 (datorklase)
8.	Neautentiska uzvedība sociālajos tīklos Neautentiskas lapas Facebook Neautentiski konti Facebook Atomatizēti konti Twitter (boti) Klikšķu fernas Troļļu fabrikas	Lekcijas	1 (datorklase)
9.	Notikuma verificācija demonstrējot pierādījumu pārbaudes metodes Semināra darbs atbilstoši semināra Nr. 3 instrukcijai.	Nodarbības	1 (datorklase)
10.	Interesu konflikta identifikācija atvērtajos datos (Vieslekcija) Uzņēmumu reģistra, KANB partiju finansēšanas, VID amatpersonu deklarāciju un iepirkumu uzraudzības biroja (IUB) publicētie u.c. dati; Gadījuma studijas ar izplatītajām korupcijas un interešu konfliktu shēmām	Lekcijas	1 (datorklase)
11.	Datu analīze Excel Datu importēšana, formatēšana, kārtošana, atlase, meklēšana; Datu kopu sapludināšana; Rakurstabulas	Nodarbības	1 (datorklase)
12.	Mājaslapu izmeklēšana Domēnu reģistrs, anonimizācijas servisi, IP adresess, VPN; SSL sertifikāti; Apmeklējumu plūsma (SmilarWeb/Alexa); Backlinks; Sīkdatnes; Source code – unikālie	Lekcijas	1 (datorklase)
13.	Tīkla analīze veicot mājaslapas izpēti Semināra darbs atbilstoši semināra Nr. 5 instrukcijai.	Nodarbības	0.5 (datorklase)
14.	Krāpniecība un noziegumi internetā (Vieslekcija) Pikšķerēšana; Identitāšu zādzība; Uzlaušana; Sociālā inženierija (izlikšanās par banku); DDoS uzbrukumi; Doksings u.c.	Lekcijas	1 (datorklase)

15.	Drošība internetā (Vieslekcija) Lietotāja identitātes aizsardzība tiešsaistē (VPN, virtuālās mašīnās; pārlūka iestatījumi) Paroļu administrēšana, divu/trīs faktoru verifikācija, biometrija; Aizsardzība pret spiegošanu caur digitālajām ierīcēm; Lokācijas servisu droša izmantošana u.c.	Lekcijas	1 (datorklase)
16.	Izmeklētāja drošība internetā Semināra darbs atbilstoši semināra Nr. 6 instrukcijai.	Nodarbības	1 (datorklase)
Kopā lekcijas			8
Kopā nodarbības			4
Kopā			12
Nepilns laiks			
Nr.	Tēma	Īstenošanas forma	Skaitis (norises vieta)
1.	Advancēta meklēšana interneta pārlūkos Interneta pārlūku dorkings: • Meklēt konkrētā lapā; • Meklēt konkrētu frāzi; • Meklēt konkrētu failu tipu; • Meklēt pēc attēla u.c. Arhivētais saturs; Personas datu meklēšana pēc personas vārda, lietotāja vārda, e-pasta, adreses, telefona numura	Lekcijas	0.5 (datorklase)
2.	Meklēšana sociālajos tīklos Facebook; Twitter; Instagram; VKo ntakte; YouTube; WhatsApp grupas; Telegram kanāli un grupas.	Lekcijas	0.5 (datorklase)
3.	Interesešu konflikta identifikācija atvērtajos datos (Vieslekcija) Uzņēmumu reģistra, KANB partiju finansēšanas, VID amatpersonu deklarāciju un iepirkumu uzraudzības biroja (IUB) publicētie u.c. dati; Gadījuma studijas ar izplatītākajām korupcijas un interesešu konfliktu shēmām	Lekcijas	0.5 (datorklase)
4.	Datu analīze Excel Datu importēšana, formatēšana, kārtošana, atlase, meklēšana; Datu kopu sapludināšana; Rakurstabulas	Nodarbības	1 (datorklase)
5.	Mājaslapu izmeklēšana Domēnu reģistrs, anonimizācijas servisi, IP adresess, VPN; SSL sertifikāti; Apmeklējumu plūsma (SmilarWeb/Alexa); Backlinks; Sīkdatnes; Source code – unikālie	Nodarbības	1 (datorklase)
6.	Drošība internetā (Vieslekcija) Lietotāja identitātes aizsardzība tiešsaistē (VPN, virtuālās mašīnās; pārlūka iestatījumi) Paroļu administrēšana, divu/trīs faktoru verifikācija, biometrija; Aizsardzība pret spiegošanu caur digitālajām ierīcēm; Lokācijas servisu droša izmantošana u.c.	Lekcijas	0.5 (datorklase)
7.	Ievads OSINT un mūsdienu interneta vidē Atvēto avotu un datu analīze jeb OSINT kā informācijas vākšanas, apkopošanas un analīzes pieeja; Interneta vietņu darbības principi – domēnu, serveru hostēšana; Veblapu indeksācija, deepweb, dark web; Sociālie tīkli – uzmanības ekonomika, influenceri Lielo datu ekonomika, mašīnmācīšanās Datu brokeri – Cambridge Analytica, OCEAN, micro targeting; Gadījumi, kad pielieto atvēto avotu izpēti. Mājas darbs: Eseja par atklātību un privātumu mūsdienu internetā	Lekcijas	0.5 (datorklase)
8.	Pierādījumu verificēšana un neautentiska uzvedība sociālajos tīklos Teksta pārbaude; Attēlu pārbaude; Video pārbaude; Lokācijas pārbaude; Neautentiskas lapas un konti Facebook; Automatizēti konti Twitter (boti); Klikšķu fermas un troļļu fabrikas. Mājas darbs: Veikt pasniedzēja iedoto "pierādījumu" pārbaudi,	Lekcijas	0.5 (datorklase)

aprakstot pārbaudes gaitu, lietotos rīkus un pamatojot secinājumus par pierādījumu autentiskumu.		
	Kopā lekcijas	3
	Kopā nodarbības	2
	Kopā	5

Vērtēšana

Patstāvīgais darbs:

1. Lekcijās un semināros izskatītais materiāls ir nepieciešamo zināšanu apguves minimums. Pārējie jautājumi, kas nav izskatīti kontaktnodarbībās, studentam jāapgūst patstāvīgi. Visi studiju kursā apgūstamie jautājumi ir norādīti kursa aprakstā.
2. Materiālu apguvei ārpusauditoriju darba laikā ir jābūt sistemātiskai. Jārēķinās, ka uz divām auditorijas stundām (90 min.) vajag paredzēt vismaz 3 stundas ārpusauditoriju darba (esejas sagatavošana/individuālā darba veikšana, gatavošanās semināriem).
3. Semināru nodarbības notiek grupās un individuāli, izmantojot personīgos klēpju datorus vai augstskolas nodrošinātus stacionāros datorus. Studenti gatavojas semināra darbam individuāli vai grupās. Detalizēta semināra darba organizācija ietverta semināra instrukcijā par attiecīgo semināru, kas nosūtīta studentiem 5 – 7 kalendārās dienas pirms semināra. Studentiem ir pienākums pirms nodarbības sagatavoties atbilstoši instrukcijā norādītajam, piemēram, iepazīties ar kādu gadījumu, kur tika izmantoti atvērtie avoti, izpētīt papildjautājumus un rast atbildes uz tiem, ja tādi uzdoti, un pēcāk seminārā – nodemonstrēt savas patstāvīgās atvērtu avotu un datu pētniecības prasmes.
4. Paralēli visiem patstāvīgajiem darbiem, katram studentam individuāli jāizstrādā atvērtu avotu pētījums (kurš darbs) par kādu konkrētā lietā aizdomās turamo individu, pārbaudot viņa alibi, sociālo kontu tīklu un mājaslapu tīklu, kas iespējams iesaistīti kādā ekonomiskā noziegumā vai iespēju robežās jāatklāj kāds noziegums, izmantojot atvērtu avotu un datu sniegtos pierādījumus.

Vērtēšanas kritēriji:

Kursa ietvaros studentiem tiks likts vērtējums par darbu semināros, kursa noslēguma darbu un eksāmenu. Vērtējuma izlikšanai nepieciešams:

- 1) Patstāvīga kursa noslēguma darba izstrāde;
- 2) Nodarbību apmeklētība un sekmīgi vērtējumi semināros;
- 3) Eksāmena sekmīga nokārtošana.

Semināru darbs – 25%,
Kursa noslēguma darbs – 50%,
Eksāmens – 25%.

Gala pārbaudījums (pilna laika studijas): Eksāmens (Rakstisks)

Gala pārbaudījums (nepilna laika studijas): Eseja par eksāmena jautājumiem (Rakstisks)

Gala pārbaudījums (pilna laika studijas): Eksāmens (Rakstisks)

Gala pārbaudījums (nepilna laika studijas): Eksāmens (Rakstisks)

Studiju rezultāti

Zināšanas:

Studenti zina atvērtu avotu izpēti (OSINT) metodes, pieejas, rīkus, izprot tiešsaistes tīklu, interneta pārlūku, mājaslapu un lielāko sociālo tīklu darbības principus, zina profesijai noderīgākās atvērtās datu bāzes, kā arī apzinās un izprot drošības riskus, ar ko sastopas interneta lietotāji, tajā skaitā pats izmeklētājs. Studiju kursa apguves rezultātā studenti spēj integrēt iegūtās zināšanas un dot ieguldījumu jaunu zināšanu radīšanā.


Prasmes:

Studenti prot meklēt un sistematizēt atvērtajos avotos pieejamos pierādījumus (tekstus, foto, video, unikālus identifikators u.tml.), lai vēlāk tos pārbaudītu, analizētu un iegūto informāciju sintezētu, izdarot secinājumus par izmeklējamā noziegumu. Izprotot interneta un sociālo tīklu darbības principus, studenti ir spējīgi izmantot pasniedzēja sniegtās zināšanas un patstāvīgi radīt jaunas atvērtu avotu pētniecības pieejas. Studenti spēj iesaistīties diskusijās par interneta un sociālo tīklu attīstību, to lietotāju privātumu, drošību, kā arī pētnieka ētiku.

Kompetences:

Studenti ir kompetenti veikt ekonomisko noziegumu izmeklēšanu, strādājot ar pierādījumiem, kas iegūti atvērtajos un publiskajos avotos, kā arī konsultēt izmeklētājus, kas izmanto citas pierādījumu vākšanas metodes.



Bibliogrāfija**Obligātā literatūra:**

Nr.	Nosaukums	Saite
1.	Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analysing Online Information. 7th Edition. Coppel, Texas, 2019	
2.	Akhgar, B., Bayerl, S., Sampson, F. Open Source Intelligence Investigation: From Strategy to Implementation. Springer International Publishing, Switzerland, 2016	
3.	Hassan, N., Hijazi, R. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress Media LLC, New York, 2018	
4.	Troia, V. Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques. John Wiley & Sons, Indianapolis, 2020	
5.	Gupta, R., Brooks, H. Using Social Media for Global Security. John Wiley & Sons, Incorporated, 2013	
6.	Orlowski, J. The Social Dilemma. Netflix, 2020	

Papildu literatūra:

Nr.	Nosaukums	Saite
1.	Amer, K., Noujaim, J. The Great Hack. Netflix 2019	
2.	Fincher, D. The Social Network. Columbia Pictures, 2010	

Citi informācijas avoti:

Nr.	Nosaukums	Saite
1.	Intel Techniques	
2.	Bellingcat	
3.	Verification and Fact Checking Handbook	