

## Studiju kursa apraksts

### Nacionālā drošība

Kursa apraksta statuss: Apstiprināts

Kursa apraksta versija: 10.00

Kursa apraksta apstiprināšanas datums: 22.04.2024 08:26:58

#### Par studiju kursu

Kursa kods:	JF_428	LKI līmenis:	7. līmenis
ECTS:	3.00	Kredītpunkti:	2.00
Zinātnes nozare:	Vadībzinātne		
Mērķauditorija:	Tiesību zinātne; Uzņēmējdarbības vadība; Vadībzinātne		

#### Studiju kursa vadītājs

Kursa vadītājs:	Vitālijs Rakstiņš
-----------------	-------------------

#### 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	6	2	12	Eksāmens (Rakstisks)	3.00
	Nodarbības	6	2	12		
	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:

Vadībzinātnē, ekonomikā, finansēs un tiesību zinātnē pamata līmenī.

##### Mērķis:

Kursa mērķis ir sniegt strukturētas zināšanas par nacionālās drošības sistēmu. Kursa gaitā studenti tiks iepazīstināti ar mūsdienu riskiem un apdraudējumiem, nacionālās drošības sistēmas tiesisko regulējumu un institucionālo ietvaru, krīzes vadību un noturības stiprināšanu. Kursa ietvaros tiks apskatīti arī šādi aktuālie drošības izaicinājumi – piegāžu drošība, ārvalstu tiešie ieguldījumi, kibernetiskā drošība un informācijas drošība, hibrīdais apdraudējums. Kursa praktiskajās nodarbībās studentiem tiks sniegtas nepieciešamās pamatzināšanas par organizācijas operacionālās drošības un darbības nepārtrauktības plānošanu, sagatavojot organizācijas drošības jeb krīzes rokasgrāmatu.

**Tēmu saraksts****Pilns laiks**

Nr.	Tēma	Īstenošanas forma	Skaitis (norises vieta)
1.	Mūsdienu riski un apdraudējumi. Nacionālā drošības sistēma. Nacionālās drošības koncepcija. Nacionālās drošības likums. Institucionālais ietvars. Ministru kabineta, Valsts Prezidenta, Saeimas, pašvaldību, dažādu institūciju un iestāžu atbildība apdraudējumu pārvarēšanā. Speciālais tiesiskais režīms: ārkārtējā situācija un izņēmuma stāvoklis. Privāto personu tiesības un pienākumi.	Lekcijas	0.25 ( auditorija )
2.	Civilās aizsardzības starptautiskais un Latvijas nacionālais tiesiskais regulējums (plānošanas dokumenti, normatīvie akti, starptautiskās konvencijas). Civilās aizsardzības sistēma. Dabas katastrofas (ģeofiziskās, hidroloģiskās, meteoroloģiskās, klimatoloģiskās, bioloģiskās, kosmiskās). Antropogēnās katastrofas (tehnogēnās katastrofas, sabiedriskās nekārtības, terora akti, iekšējie nemieri). Valsts institūciju, pašvaldību un komersantu pienākumi un tiesības. Civilās aizsardzības komisijas. Civil	Lekcijas	0.75 ( auditorija )
3.	Terorisms un radikalizācija. Vēsturiskais ieskats, apdraudējuma apraksts, terorisma definīcijas, mūsdienu tendences. Eiropas Savienības pretterorisma rīcības dokumenti. Nacionālā pretterorisma sistēma. Terorisma draudu līmeni. Terorisma finansēšanas un atbalstīšanas novēršanas pasākumi. Prekursoru kontrole. Mūsdienu tehnoloģiju izaicinājumi. Preventīvie pasākumi. Izaicinājumi interneta vidē, radikalizācija un konvertācija sociālajos tīklos un internetā.	Lekcijas	0.5 ( auditorija )
4.	Praktiskā nodarbība atbilstoši instrukcijai Nr.1 un 2: iepriekš izvēlētās organizācijas risku novērtējums un risku pārvaldīšanas sistēmas vai organizācijas civilā aizsardzības plāna apraksta prezentācija.	Nodarbības	1 (auditorija)
5.	Privātā sektora loma nacionālajā drošības sistēmā. Ārvalstu pieredze (dažādu valstu modeļu apskats: visas sabiedrības iesaiste; totālā aizsardzība; drošības funkciju deleģēšana privātajam sektoram). Latvijas normatīvais regulējums un pieredze. Visaptveroša valsts aizsardzība. COVID19 (SARS-CoV-2). Latvijas iekšējā drošība –normatīvais regulējums un institucionālais ietvars. Kritiskā infrastruktūra. Kritiskie finanšu pakalpojumi. Pamatpakalpojumu sniedzēji. Industriālās drošības sertifikāts.	Lekcijas	0.5 ( auditorija )
6.	Tests Nr.1 (jautājumi par tēmām: nacionālās drošības sistēma, institūcijas un to loma, krīzes vadība, civilās aizsardzības sistēma, dažādu katastrofu pārvaldība, pretterorisma pasākumi).	Nodarbības	1 (auditorija)

7.	Kiberdrošība. Riski un apdraudējumi digitālajā vidē, kiberuzbrukumi un kibernetizācija. Kibersankcijas. Eiropas Savienības regulējums un iniciatīvas. Nacionālā kiberdrošības ekosistēma, normatīvais regulējums un institucionālais ietvars. CERT.lv. Kiberdrošības pamati / kiberhigiēna. Standartu ģimene ISO 27000. Rīcība kiberuzbrukumu gadījumā. Atbildīgā atklāšana. 5G izaicinājumi. Lietu interneta ievainojamības. Kiberaizsardzība un kiberkarš. Nākotnes riski.	Lekcijas	0.5 ( auditorija )
8.	Apdraudējumi informatīvajā telpā. Informatīvās telpas drošība. Dezinformācija un informācijas operācijas. Sociālo mediju algoritmi. Radikalizācija. Psiholoģiskā noturība. Medijprasmes. Reputācijas riski.	Lekcijas	0.25 ( auditorija )
9.	Datu drošība. Apdraudējumi. Kontrole par saviem datiem. GDPR. Datu ekonomika. Lielie dati. Dati un mākslīgais intelekts. Datu brokeri. Organizācijas un personīgas informācijas drošība. Datu integritāte, konfidencialitāte un pieejamība.	Lekcijas	0.25 ( auditorija )
10.	Kiberhigiēnas un informācijas drošības tests, kam sekos kļūdu analīze, lai sekmētu izglītojamo spējas mazināt savas un savas organizācijas ievainojamības digitālajā vidē un pilnveidot kiberdrošības prasmes.	Nodarbības	0.5 (auditorija)
11.	Praktiskā nodarbība atbilstoši instrukcijai Nr.3 un Nr. 4: Organizācijas kiberdrošības pasākumu plānošana un organizācijas objekta fiziskās apsardzes plānošana.	Nodarbības	0.5 (auditorija)
12.	Hibrīdais apdraudējums (teorija, definīcijas, vēsturiskais ieskaits). Hibrīda apdraudējuma veidi, metodes, tendences. Riski "pelēkajā zonā". Starptautisko organizāciju un ārvalstu pieredze, rīcība un plāni. Noturības stiprināšana kā atbilde uz hibrīdo apdraudējumu. Latvijas normatīvais regulējums un institucionālais ietvars.	Lekcijas	0.5 ( auditorija )
13.	Militārais apdraudējums (apdraudējuma apraksts, vēsturisks ieskaits, konvencijas, izaicinājumi). Valsts aizsardzības sistēma (vēsturiskais ieskaits, pamata dokumenti, obligātais militārais dienests, izmaiņas pēc iestāšanās NATO). Valsts aizsardzības koncepcija. Nacionālie bruņotie spēki. Zemessardze. Rezerves karavīri. Rezervisti. Izņēmuma stāvoklis un kara laiks. NATO Vašingtonas līguma 5.pants. Sabiedrotie. Uzņemotās valsts atbalsta sniegšana. Mobilizācijas sistēma.	Lekcijas	0.5 ( auditorija )
14.	Ilgtermiņa (fokuss uz ilgtermiņa risku novērtējumu). ANO Ilgtspējīgas attīstības 17 mērķi (Dienaskārtība 2030). ES "zaļā kursa" iniciatīvas. OECD vadlīnijas multinacionālajiem uzņēmumiem. ANO Vadošie principi uzņēmējdarbībai un cilvēktiesībām. Sociāli korporatīvā atbildība un ESG (Environmental. Social. Governance). Ētikas dilemmas. Ilgtermiņa risku novērtējums kā pamats uzņēmuma ilgtspējībai. Noturības un darbības nepārtrauktības plānošana. Adaptācija klimata pārmaiņām. Risku izvērtēšana.	Nodarbības	0.5 (auditorija)
15.	Tests Nr.2 (jautājumi par tēmām: hibrīda apdraudējums, kiberdrošība, informācijas drošība, militārais apdraudējums, karš).	Nodarbības	0.5 (auditorija)

16.	<p>Ekonomiskā un finanšu drošība. Ārvalstu tiešās investīcijas un ieguldījumi no drošības viedokļa. Citi veidi kā iegūt būtisko ietekmi organizācijā. Riski zinātnē un pētniecībā. Rūpnieciskā spiegošana. Ārvalstu pieredze un ES iniciatīvas. Nacionālās drošības likums. Piegāžu drošības riski. Piegādātāju riski. Piegāžu ķēdes novērtējums un monitorings. Starptautiskās un Latvijas Republikas sankcijas. Piegādātāju atbilstība korporatīvās pārvaldības prasībām (CSR, ESG).</p>	Lekcijas	1 ( auditorija )
17.	<p>Organizācijas darbības nepārtrauktības plānošana un krīzes vadība. Kritiskās funkcijas. Kritiskais personāls, IT sistēmas un infrastruktūra. Darbības nepārtrauktības plānošana. Starptautiskais standarts ISO 22301:2019 un citi standarti. Organizācijas operacionālās noturības stiprināšana, tostarp izvēloties piegādātājus, investorus un sadarbības partnerus. Nacionālās drošības likums. Kritisko funkciju nepārtrauktības nodrošināšana. Krīzes vadība. Krīzes komunikācija un informācijas aprīte.</p>	Lekcijas	1 ( auditorija )
18.	<p>Katra studenta patstāvīga kursa noslēguma darba (organizācijas drošības rokasgrāmatas izstrādātas pēc instrukcijām Nr.1-5) prezentācija. Uz nodarbību nepieciešams sagatavot arī organizācijas darbības nepārtrauktības plānu atbilstoši instrukcijai Nr.5.</p>	Nodarbības	2 (auditorija)
<b>Kopā lekcijas</b>			6
<b>Kopā nodarbības</b>			6
<b>Kopā</b>			12
<b>Nepilns laiks</b>			
Nr.	Tēma	Īstenošanas forma	Skaits (norises vieta)
1.	<p>Mūsdienu riski un apdraudējumi. Nacionālā drošības sistēma. Nacionālās drošības koncepcija. Nacionālās drošības likums. Institucionālais ietvars. Ministru kabineta, Valsts Prezidenta, Saeimas, pašvaldību, dažādu institūciju un iestāžu atbildība apdraudējumu pārvarēšanā. Speciālais tiesiskais režīms: ārkārtējā situācija un izņēmuma stāvoklis. Privāto personu tiesības un pienākumi.</p>	Lekcijas	0.25 ( auditorija )
2.	<p>Civilās aizsardzības starptautiskais un Latvijas nacionālais tiesiskais regulējums (plānošanas dokumenti, normatīvie akti, starptautiskās konvencijas). Civilās aizsardzības sistēma. Dabas katastrofas (ģeofiziskās, hidroloģiskās, meteoroloģiskās, klimatoloģiskās, bioloģiskās, kosmiskās). Antropogēnās katastrofas (tehnogēnās katastrofas, sabiedriskās nekārtības, terora akti, iekšējie nemieri). Valsts institūciju, pašvaldību un komersantu pienākumi un tiesības. Civilās aizsardzības komisijas. Civil</p>	Lekcijas	0.25 ( auditorija )
3.	<p>Terorisms un radikalizācija. Vēsturiskais ieskats, apdraudējuma apraksts, terorisma definīcijas, mūsdienu tendences. Eiropas Savienības pretterorisma rīcības dokumenti. Nacionālā pretterorisma sistēma. Terorisma draudu līmeni. Terorisma finansēšanas un atbalstīšanas novēršanas pasākumi. Prekursoru kontrole. Mūsdienu tehnoloģiju izaicinājumi. Preventīvie pasākumi. Izaicinājumi interneta vidē, radikalizācija un konvertācija sociālajos tīklos un internetā.</p>	Lekcijas	0.25 ( auditorija )

4.	Praktiskā nodarbība atbilstoši instrukcijai Nr.1 un 2: iepriekš izvēlētās organizācijas risku novērtējums un risku pārvaldīšanas sistēmas vai organizācijas civilā aizsardzības plāna apraksta prezentācija.	Nodarbības	0.5 (auditorija)
5.	Privātā sektora loma nacionālajā drošības sistēmā. Ārvalstu pieredze (dažādu valstu modeļu apskats: visas sabiedrības iesaiste; totālā aizsardzība; drošības funkciju deleģēšana privātajam sektoram). Latvijas normatīvais regulējums un pieredze. Visaptveroša valsts aizsardzība. COVID19 (SARS-CoV-2). Latvijas iekšējā drošība –normatīvais regulējums un institucionālais ietvars. Kritiskā infrastruktūra. Kritiskie finanšu pakalpojumi. Pamatpakalpojumu sniedzēji. Industriālās drošības sertifikāts.	Lekcijas	0.1 ( auditorija )
6.	Tests Nr.1 (jautājumi par tēmām: nacionālās drošības sistēma, institūcijas un to loma, krīzes vadība, civilās aizsardzības sistēma, dažādu katastrofu pārvaldība, pretterorisma pasākumi).	Nodarbības	0.5 (auditorija)
7.	Kiberdrošība. Riski un apdraudējumi digitālajā vidē, kiberuzbrukumi un kibernetizācija. Kibersankcijas. Eiropas Savienības regulējums un iniciatīvas. Nacionālā kiberdrošības ekosistēma, normatīvais regulējums un institucionālais ietvars. CERT.lv. Kiberdrošības pamati / kiberhigiēna. Standartu ģimene ISO 27000. Rīcība kiberuzbrukumu gadījumā. Atbildīgā atklāšana. 5G izaicinājumi. Lietu interneta ievainojamības. Kiberaizsardzība un kiberkarš. Nākotnes riski.	Lekcijas	0.25 ( auditorija )
8.	Apdraudējumi informatīvajā telpā. Informatīvās telpas drošība. Dezinformācija un informācijas operācijas. Sociālo mediju algoritmi. Radikalizācija. Psiholoģiskā noturība. Medijprasmes. Reputācijas riski.	Lekcijas	0.1 ( auditorija )
9.	Datu drošība. Apdraudējumi. Kontrole par saviem datiem. GDPR. Datu ekonomika. Lielie dati. Dati un mākslīgais intelekts. Datu brokeri. Organizācijas un personīgas informācijas drošība. Datu integritāte, konfidencialitāte un pieejamība.	Lekcijas	0.1 ( auditorija )
10.	Kiberhigiēnas un informācijas drošības tests, kam sekos kļūdu analīze, lai sekmētu izglītojamo spējas mazināt savas un savas organizācijas ievainojamības digitālajā vidē un pilnveidot kiberdrošības prasmes.	Nodarbības	0.25 (auditorija)
11.	Praktiskā nodarbība atbilstoši instrukcijai Nr.3 un Nr. 4: Organizācijas kiberdrošības pasākumu plānošana un organizācijas objekta fiziskās apsardzes plānošana.	Nodarbības	0.25 (auditorija)
12.	Hibrīdais apdraudējums (teorija, definīcijas, vēsturiskais ieskats). Hibrīda apdraudējuma veidi, metodes, tendences. Riski "pelēkajā zonā". Starptautisko organizāciju un ārvalstu pieredze, rīcība un plāni. Noturības stiprināšana kā atbilde uz hibrīdo apdraudējumu. Latvijas normatīvais regulējums un institucionālais ietvars.	Lekcijas	0.1 ( auditorija )

13.	Militārais apdraudējums (apdraudējuma apraksts, vēsturisks ieskaits, konvencijas, izaicinājumi). Valsts aizsardzības sistēma (vēsturiskais ieskaits, pamata dokumenti, obligātais militārais dienests, izmaiņas pēc iestāšanās NATO). Valsts aizsardzības koncepcija. Nacionālie bruņotie spēki. Zemessardze. Rezerves karavīri. Rezervisti. Izņēmuma stāvoklis un kara laiks. NATO Vašingtonas līguma 5.pants. Sabiedrotie. Uzņemšanās valsts atbalsta sniegšana. Mobilizācijas sistēma.	Lekcijas	0.25 ( auditorija )
14.	Ilgtermiņa (fokuss uz ilgtermiņa risku novērtējumu). ANO Ilgtspējīgas attīstības 17 mērķi (Dienaskārtība 2030). ES “zaļā kursa” iniciatīvas. OECD vadlīnijas multinacionālajiem uzņēmumiem. ANO Vadošie principi uzņēmējdarbībai un cilvēktiesībām. Sociāli korporatīvā atbildība un ESG (Environmental. Social. Governance). Ētikas dilemmas. Ilgtermiņa risku novērtējums kā pamats uzņēmuma ilgtspējībai. Noturības un darbības nepārtrauktības plānošana. Adaptācija klimata pārmaiņām. Risku izvērtēšana.	Nodarbības	0.1 (auditorija)
15.	Tests Nr.2 (jautājumi par tēmām: hibrīda apdraudējums, kibernetiskā drošība, informācijas drošība, militārais apdraudējums, karš).	Nodarbības	0.1 (auditorija)
16.	Ekonomiskā un finanšu drošība. Ārvalstu tiešās investīcijas un ieguldījumi no drošības viedokļa. Citi veidi kā iegūt būtisko ietekmi organizācijā. Riski zinātnē un pētniecībā. Rūpnieciskā spiegošana. Ārvalstu pieredze un ES iniciatīvas. Nacionālās drošības likums. Piegāžu drošības riski. Piegādātāju riski. Piegāžu ķēdes novērtējums un monitorings. Starptautiskās un Latvijas Republikas sankcijas. Piegādātāju atbilstība korporatīvās pārvaldības prasībām (CSR, ESG).	Lekcijas	0.75 ( auditorija )
17.	Organizācijas darbības nepārtrauktības plānošana un krīzes vadība. Kritiskās funkcijas. Kritiskais personāls, IT sistēmas un infrastruktūra. Darbības nepārtrauktības plānošana. Starptautiskais standarts ISO 22301:2019 un citi standarti. Organizācijas operacionālās noturības stiprināšana, tostarp izvēloties piegādātājus, investorus un sadarbības partnerus. Nacionālās drošības likums. Kritisko funkciju nepārtrauktības nodrošināšana. Krīzes vadība. Krīzes komunikācija un informācijas aprīte.	Lekcijas	0.6 ( auditorija )
18.	Katra studenta patstāvīga kursa noslēguma darba (organizācijas drošības rokasgrāmatas izstrādātas pēc instrukcijām Nr.1-5) prezentācija. Uz nodarbību nepieciešams sagatavot arī organizācijas darbības nepārtrauktības plānu atbilstoši instrukcijai Nr.5.	Nodarbības	0.3 (auditorija)
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. Studenti gatavojas individuāli semināra darbam. 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, izpētīt papildjautājumus un rast atbildes uz tiem, ja tādi uzdoti, un pēcāk seminārā – prast aizstāvēt savu viedokli un pamatot to diskusijās ar citiem studentiem.

#### **Vērtēšanas kritēriji:**

Kursa ietvaros studentiem tiks organizēti divi testi, par kuriem studenti saņem vērtējumu, tāpat vērtējums tiek likts par darbu semināros, kursa noslēguma darbu un gala eksāmenu. Vērtējuma izlikšanai nepieciešams:

- 1) Patstāvīga kursa noslēguma darba (organizācijas drošības rokasgrāmatas) izstrāde.
- 2) Nodarbību apmeklētība un sekmīgi vērtējumi semināros.
- 3) Divi testu un eksāmena sekmīga nokārtošana.

Patstāvīga gatavošanās semināriem un aktīva dalība nodarbībās, t.sk. divas prezentācijas – 30%,  
Kursa noslēguma darbs – 30%,  
Divi pārbaudes testi un gala eksāmens – 40%.

<b>Gala pārbaudījums (pilna laika studijas):</b>	Eksāmens (Rakstisks)
--	----------------------

<b>Gala pārbaudījums (nepilna laika studijas):</b>	Eksāmens (Rakstisks)
--	----------------------

#### **Studiju rezultāti**

##### **Zināšanas:**

Izprot mūsdienu apdraudējumus un nacionālo drošības sistēmu, pārzina tiesisko regulējumu un standartus, un aktuālās attīstības tendences, krīzes vadības un noturības pamatus, orientējas sabiedrības ilgtspējīgas attīstības principos. Ir iegūtas padziļinātas zināšanas par nozaru apdraudējumu pārvaldību un iesaistīto institūciju sadarbību krīzes situācijās. Ir izveidojies priekšstats par organizācijas drošību (pamata zināšanas par risku vadību, civilo aizsardzību, fizisko drošību, kiberdrošību, darbības nepārtrauktības plānošanu).

##### **Prasmes:**

Studenti demonstrē prasmi domāt organizācijas drošības kategorijās, spēj patstāvīgi iegūt un apkopot informāciju, analizēt riskus un prognozēt cēloņsakarības, sagatavot nepieciešamos dokumentus, pārskatus, prezentācijas un publikācijas. Studenti spēj argumentēti diskutēt par nacionālās drošības jautājumiem un mūsdienu apdraudējumiem. Spēj pielietot iegūtās zināšanas un prasmes plānojot organizācijas operacionālo drošību un darbības nepārtrauktību, kā arī risināt ar specializētiem pētījumiem un inovācijām saistītas problēmas.

##### **Kompetences:**

Studenti ir kompetenti risināt augstās komplicētības pakāpes jautājumus un nodrošināt uz risku novērtējumu balstīto lēmumu pieņemšanu drošības jomā. Spēj efektīvi izmantot organizācijas resursus, maksimizējot organizācijas un sabiedrības ieguvumus. Spēj integrēt dažādu jomu zināšanas, dodot ieguldījumu jaunu zināšanu radīšanā.

#### **Bibliogrāfija**

##### **Obligātā literatūra:**



Nr.	Nosaukums	Saite
1.	Nacionālās drošības koncepcija (apstiprināta Saeimā 28.09.2023)	
2.	Valsts aizsardzības koncepcija (apstiprināta Saeimā 05.10.2023)	
3.	Latvijas kiberdrošības stratēģija 2023. – 2026. gadam (apstiprināta MK 28.03.2023)	
4.	Ministru kabineta 2018.gada informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanu Latvijā" (2018.gada VSS-846)	
5.	Nacionālās drošības likums	
6.	Likums "Par ārkārtējo situāciju un izņēmuma stāvokli"	
7.	Ārvalstu studentiem/For international students	
8.	National Security Law	




9.	Mobilisation Law	
10.	Military Service Law	
11.	RAND research: Deterring Russian Aggression in the Baltic States Through Resilience and Resistance. 2019.	<a href="#">🔗</a>
12.	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Michael N. Schmitt, Cambridge University Press, 2017.	
13.	Until Something Moves: Reinforcing the Baltic Region in Crisis and War. Ben Hodges, Tony Lawrence, Ray Wojcik. ICDS /CEPA. 2020. 40.lpp.	
14.	Valsts aizsardzības dienesta likums	
15.	Valsts Civilās aizsardzības plāns (2024.g.)	
16.	Ministru kabineta 2021.gada 6.jūlija noteikumi Nr.508 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtība"	

#### Papildu literatūra:

Nr.	Nosaukums	Saite
1.	Latvijas Republikas Satversmes komentāri. III nodaļa. Valsts prezidents. IV nodaļa. Ministru kabinets. Sagatavojis autoru kolektīvs. Rīgā: Latvijas vēstnesis. 2017. 864.lpp.	
2.	World-Class Risk Management. Norman Marks. 2015. 236.lpp.	
3.	The Failure of Risk Management: Why It's Broken and How to Fix It, 2nd Edition. Douglas W. Hubbard. 2019. 336.lpp.	
4.	Towards #NATO2030: The Regional Perspective of the Baltic States and Poland. Māris Andžāns, Mārtiņš Vargulis. Latvian Institute of International Affairs, 2020. 209.lpp.	
5.	Jurista Vārda" grāmatžurnāls. Dati kā tehnoloģiju laikmeta resursi: izmantošana un aizsardzība. Latvijas vēstnesis. 2020. 120.lpp.	
6.	OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity. 2015. Pieejāms OECD mājaslapā.	
7.	VUGD. Par Latvijas risku novērtēšanas kopsavilkums. Informatīvais ziņojums, Valsts Ugunsdzēsības un glābšanas dienests, Rīgā, 2015.	
8.	Ministru kabineta 2019.gada 17.jūlija rīkojums Nr.380 Plāns "Latvijas pielāgošanās klimata pārmaiņām plāns laika posmam līdz 2030. gadam"	
9.	VARAM pētījums "Risku un ievainojamības novērtējums un pielāgošanās pasākumu identificēšana civilās aizsardzības un ārkārtas palīdzības jomā" (2016.-2017.g.).	<a href="#">🔗</a>
10.	1977.gada 8.jūnija papildu protokols pie 1949.gada 12.augusta Ženēvas konvencijām, kas attiecas uz starptautiska rakstura bruņotu konfliktu upuru aizsardzību (I protokols)	
11.	1977.gada 8.jūnija papildu protokols pie 1949.gada 12.augusta Ženēvas konvencijām, kas attiecas uz lokāla rakstura bruņotu konfliktu upuru aizsardzību (II protokols)	
12.	Eiropas Komisija. "Risku novērtēšanas un kartēšanas vadlīnijas katastrofu pārvaldībai". Komisijas dienestu darba dokuments. SEC(2010) 1626 galīgā redakcija. Brisele. 2010.	<a href="#">🔗</a>
13.	ES pretterorisma plānošanas dokuments: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. 2020.	
14.	Ministru kabineta 2017.gada 7.novembra noteikumi Nr.658 "Noteikumi par civilās aizsardzības plānu struktūru un tajos iekļaujamo informāciju"	
15.	Ministru kabineta 2016.gada 1.marta noteikumi Nr.131 "Rūpniecisko avāriju riska novērtēšanas kārtība un riska samazināšanas pasākumi"	



16.	Ministru kabineta 2006.gada 18.aprīļa noteikumi Nr.290 "Kārtība, kādā sabiedriskās kārtības un drošības interesēs var pieprasīt gaisa kuģa piespiedu nosēdināšanu un kādā tiek pieņemts lēmums par kaujas darbību veikšanu pret gaisa kuģi Latvijas Republikas teritorijā"	
17.	Ministru kabineta 2017.gada 8.augusta noteikumi Nr.440 "Valsts agrīnās brīdināšanas sistēmas izveidošanas, darbības un finansēšanas kārtība"	
18.	Ministru kabineta 2017. gada 19. septembra noteikumi Nr. 563 "Paaugstinātas bīstamības objektu apzināšanas un noteikšanas, kā arī civilās aizsardzības un katastrofas pārvaldīšanas plānošanas un īstenošanas kārtība"	
19.	Terorisma finansēšanas novēršanas stratēģija 2019.-2021.g. VDD, 2019.	
20.	Ministru kabineta 2009.gada 28.aprīļa noteikumi Nr.365 "Noteikumi par pasta, radio, televīzijas un citu plašsaziņas līdzekļu darba nodrošināšanu valsts apdraudējuma gadījumā"	
21.	OECD Good governance for critical infrastructure resilience. 2020. Pieejams OECD mājaslapā.	
22.	OECD Recommendation on the Governance of Critical Risks. 2014. Pieejams OECD mājaslapā	
23.	Ministru kabineta 2002.gada 19.marta noteikumi Nr.127 "Epizootiju uzliesmojuma likvidēšanas un draudu novēršanas kārtība"	
24.	NATO stratēģiskā koncepcija. 2022.	
25.	Ministru kabineta 2003.gada 8.aprīļa noteikumi Nr.152 "Prasības attiecībā uz sagatavošanos radiācijas avārijai un rīcību šādas avārijas gadījumā".	
26.	Ministru kabineta 2005.gada 8.novembra noteikumi Nr.837 "Noteikumi par mobilizācijas gatavības pārbaudēm un mobilizācijas mācībām"	
27.	Ministru kabineta 2010.gada 21.maija rīkojums Nr.283 "Par Nacionālo gatavības plānu naftas, bīstamo vai kaitīgo vielu piesārņojuma gadījumiem jūrā"	
28.	Eiropas Parlamenta un Padomes 2019.gada 19.marta regula Nr. 2019/452 ar ko izveido regulējumu ārvalstu tiešo ieguldījumu Savienībā izvērtēšanai	
29.	Eiropas komisijas paziņojums. Ārvalstu tiešo ieguldījumu veicināšana, vienlaikus aizsargājot būtiskas intereses. Briselē, 13.9.2017.	
30.	Ministru kabineta 2011.gada 12.aprīļa noteikumi Nr. 286 "Kārtība, kādā komersanti nodrošina un sniedz drošības rezervju pakalpojumu valsts naftas produktu drošības rezervju izveidei noteiktā apjomā" nosaka kārtību, kādā komersanti nodrošina un sniedz drošības rezervju pakalpojumu	
31.	Starptautiskais standarts ISO 22301:2019 Security and resilience. Business continuity management systems.	
32.	2015.gada ANO Ģenerālās asamblejas rezolūcija "Mūsu pasaules pārveidošana: Ilgtspējīgas attīstības programma 2030.gadam"	
33.	ANO Vadošie principi uzņēmējdarbībai un cilvēktiesībām. ANO Cilvēktiesību padomes 2011. gada 16. jūnija rezolūcija Nr.17/4	
34.	Likums "Par aviāciju"	
35.	Likums "Par radiācijas drošību un kodoldrošību"	
36.	Ministru kabineta 2017. gada 7. marta noteikumi Nr. 131 "Noteikumi par juridiskās vai fiziskās personas resursu iesaistīšanu reaģēšanas un seku likvidēšanas pasākumos vai ugunsgrēka dzēšanā, vai glābšanas darbos, kā arī tai radušos izdevumu un zaudējumu kompensācijas aprēķināšanas kārtību"	
37.	Pettere G. Riski uzņēmējdarbībā un to vadība. Rīga: Banku Augstskola, 2004. 175 lpp.	
38.	Nordic Societal Security. Sebastian Larsson & Mark Rhinard. London: Routledge, 2020. 268.lpp.	
39.	OECD Guidelines for Multinational Enterprises. 2011. Pieejams OECD mājaslapā	

40.	Agreement between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces (NATO SOFA) London, 19 June, 1951.	
41.	Making Critical Infrastructure Resilient: Ensuring Continuity of Service - Policy and Regulations in Europe and Central Asia. United Nations Office for Disaster Risk Reduction. 2020.	
42.	Ministru kabineta 2015.gada 3.marta instrukcija Nr.2. Par uzņemošās valsts atbalsta nodrošināšanu	
43.	Ministru kabineta 2015.gada 22.decembra noteikumi Nr.755 "Noteikumi par iedzīvotāju nodrošināšanu ar pirmās nepieciešamības rūpniecības precēm valsts apdraudējuma gadījumā"	
44.	Valsts katastrofu medicīnas plāna pamatdokuments. 2020.	
45.	Ministru kabineta 2007.gada 28.augusta noteikumi Nr.585 "Noteikumi par iedzīvotāju nodrošināšanu ar pārtiku valsts apdraudējuma gadījumā"	
46.	ES kiberdrošības stratēģija digitālajai desmitgadei. 2020.	
47.	Ministru kabineta 2005.gada 22.novembra noteikumi Nr.873 "Noteikumi par mobilizācijas pieprasījumiem"	
48.	Ministru kabineta 2008.gada 5.augusta instrukcija Nr.12 "Instrukcija par atbildīgo institūciju rīcību nezināmas izcelsmes vielas vai priekšmeta atrašanas gadījumā, ja ir aizdomas, ka tas satur sprādzienbīstamas, radioaktīvas, bīstamas ķīmiskas vai bioloģiskas vielas, kā arī ja konstatētas terora akta pazīmes"	
49.	Ministru kabineta 2007.gada noteikumi Nr.485 "Terorisma draudu līmeņa izsludināšanas kārtība"	
50.	ES Drošības savienības stratēģija 2020.-2025. 2020.	
51.	Sendai katastrofu risku mazināšanas ietvarprogramma 2015.-2030.gadam. Sendai Framework for Disaster Risk Reduction 2015-2030. The United Nations office for disaster risk reduction. UNISDR, 2015.	
52.	Ministru kabineta 2020.gada 26.augusta rīkojums Nr.476 "Civilās aizsardzības plāns"	
53.	Ministru kabineta 2011.gada 1.februāra noteikumi Nr.100 „Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība"	
54.	Likums "Latvijas Nacionālo bruņoto spēku piedalīšanās starptautiskajās operācijās"	
55.	Likums "Ārvalstu bruņoto spēku statuss Latvijas Republikā"	
56.	Militārā dienesta likums	
57.	Ministru kabineta 2010.gada noteikumi Nr.496 "Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība"	
58.	Latvijas Republikas Zemessardzes likums	
59.	Nacionālo bruņoto spēku likums	
60.	Mobilizācijas likums	
61.	Valsts materiālo rezervju likums	
62.	Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"	
63.	Informācijas tehnoloģiju drošības likums	
64.	Civilās aizsardzības un katastrofas pārvaldības likums	
65.	Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. ENISA, 2019.	
66.	Ārvalstu studentiem/For international students	
67.	World-Class Risk Management. Norman Marks. 2015. 236.lpp.	

68.	The Failure of Risk Management: Why It's Broken and How to Fix It, 2nd Edition. Douglas W. Hubbard. 2019. 336.lpp.	
69.	Until Something Moves: Reinforcing the Baltic Region in Crisis and War. Ben Hodges, Tony Lawrence, Ray Wojcik. ICDS /CEPA. 2020. 40.lpp.	
70.	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Michael N. Schmitt, Cambridge University Press, 2017.	
71.	Agreement between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces (NATO SOFA) London, 19 June, 1951.	
72.	Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. ENISA, 2019.	<a href="#">🔗</a>
<b>Citi informācijas avoti:</b>		
Nr.	Nosaukums	Saite
1.	Ārlietu ministrijas sagatavota informācija par bruņojuma kontroli.	<a href="#">🔗</a>
2.	Buklets "Kā rīkoties krīzes situācijā?"	<a href="#">🔗</a>
3.	Padomes Direktīva 2009/119/EK ( 2009. gada 14. septembris ), ar ko dalībvalstīm uzliek pienākumu uzturēt jēlnaftas un/vai naftas produktu obligātas rezerves	
4.	Materiāls par kiberdrošību.	<a href="#">🔗</a>
5.	LVĢMC ziņojums "Klimata pārmaiņu scenāriji Latvijai". 2017.	<a href="#">🔗</a>
6.	Hibrīda apdraudējuma izcilības centra dažādi pētījumi, raksti un analīzes par hibrīda apdraudējumu.	<a href="#">🔗</a>
7.	Kiberaizsardzības izcilības centra dažādi pētījumi, raksti un analīzes par kiberdrošību.	<a href="#">🔗</a>
8.	Stratēģiskās komunikācijas izcilības centra pētījumi, raksti un analīzes par informācijas operācijām, propagandu un datiem	<a href="#">🔗</a>
9.	European Union Agency for Cybersecurity (ENISA) materiāli par kiberdrošību	<a href="#">🔗</a>
10.	Bērziņa, I., Zupa, U. Pētījums: Latvijas sabiedrības griba aizstāvēt valsti: veicinošie un kavējošie faktori. 2020. NAA. 30.lpp.	<a href="#">🔗</a>
11.	Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā	
12.	EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019.	
13.	European Commission and High Representative of the Union for Foreign Affairs and Security Policy. "Joint Communication to the European Parliament and the Council on the Action Plan for Military Mobility." JOIN(2018) 5 final, 28 March 2018.	
14.	Roepke, Wolf-Diether and Hasit Thankey. "Resilience: the first line of defence." NATO Review, 27 February 2019.	<a href="#">🔗</a>
15.	Relationships between the economy and national security. Analysis and considerations for economic security policy in the Netherlands. RAND Corporation. 2020. 182.lpp.	<a href="#">🔗</a>
16.	How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World. White House Office of Trade and Manufacturing. 2018.	<a href="#">🔗</a>
17.	Ārvalstu studentiem/For international students	
18.	EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019.	

19.	European Commission and High Representative of the Union for Foreign Affairs and Security Policy. "Joint Communication to the European Parliament and the Council on the Action Plan for Military Mobility." JOIN(2018) 5 final, 28 March 2018.	
20.	Roepke, Wolf-Diether and Hasit Thankey. "Resilience: the first line of defence." NATO Review, 27 February 2019.	
21.	Relationships between the economy and national security. Analysis and considerations for economic security policy in the Netherlands. RAND Corporation. 2020. 182.lpp.	
22.	How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World. White House Office of Trade and Manufacturing. 2018.	