STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
KIBERNETINIS SAUGUMAS IR VERSLO ATITIKTIS	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: dr. Miglė Žukauskaitė-Tatorė **Kitas (-i):**	Vilniaus universitetas, Teisės fakultetas, Privatinės teisės katedra Saulėtekio al. 9, I rūmai, LT-10222, Vilnius 311 kab., tel. (8 5) 2366170, el. paštas: ptkatedra@tf.vu.lt

Studijų pakopa	Dalyko (modulio) tipas
Antroji	Privalomasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	9 (rudens) semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Studentai turi būti įsisavinę privalomus pirmosios pakopos teisės studijų programos dalykus; anglų kalbos mokėjimas (rekomenduojamas)	**Gretutiniai reikalavimai (jei yra):** nėra

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	133	32	101

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Dalyko tikslas - suteikti bazinių žinių apie informacinių ir komunikacijos technologijų infrastruktūros bei internetinės erdvės veikimo principus bei svarbiausius interneto infrastuktūros rinkos dalyvius, kibernetinių atakų ir pažeidžiamumų sampratą; užtikrinti studentų gebėjimą sistemiškai analizuoti verslo subjektų ir institucijų pareigas kibernetiniam saugumui užtikrinti ir šių pareigų nesilaikymo teisines pasekmes bei pagrindinių kibernetinį saugumą padedančių užtikrinti institucijų ir teisinių instrumentų funkcijas; analizuoti kibernetinio saugumo grėsmes ir reguliacines jų valdymo bei atitikties užtikrinimo strategijas, klasifikuoti nusikalstamas veikas kibernetinėje erdvėje; ugdyti gebėjimą kritiškai vertinti interneto globalumo bei tarpvalstybiškumo keliamus teisinius iššūkius.		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
Studentai suvoks interneto bei informacinių ir komunikacijos technologijų infrastuktūrą, gebės įvardinti jos rūšis ir svarbiausias funkcijas, kibernetinių rizikų įvairovę, pagrindinius jų kilmės šaltinius bei šių rizikų sukėlėjų tipus.	Paskaitos (probleminis dėstymas), seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas (informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.
Studentai gebės sistemiškai analizuoti kibernetinio saugumo reguliacinę aplinką, gerąsias rinkos praktikas bei taikomas rizikos valdymo strategijas nacionaliniu ir ES lygmeniu ir gebės jas pritaikyti praktinėse situacijose.	Paskaitos (probleminis dėstymas), seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas (informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.
Studentai, remdamiesi taikomais teisės aktais bei geraja kibernetinio saugumo užtikrinimo praktika, gebės parengti verslo subjektų atitikties kibernetinio saugumo reikalavimams programą, išskirti efektyvius kibernetinių rizikų valdymo būdus, argumentuotai konsultuoti dėl verslo	Paskaitos (probleminis dėstymas), seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.

subjektų ir institucijų pareigų bei jų nesilaikymo teisinių ir praktinių pasekmių, susijusių rizikų valdymo bei teisės aktų reikalavimus atitinkančio veiksmų plano įvykus kibernetinėms atakoms ar identifikavus sistemų pažeidžiamumus, teikti tinkamai pagrįstas rekomendacijas nuo kibernetinių atakų nukentėjusiems subjektams apie galimus jų interesų gynybos būdus.	(informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	
Studentai gebės vertinti institucijų tarptautinio bendradarbiavimo kibernetinio saugumo kontekste galimybes, išmanys svarbiausius tarptautinius instrumentus, šiuose instrumentuose numatytas pareigas ir procesus įgyvendinančius subjektus, šių instrumentų taikymo pagrindus ir prielaidas, gebės šias žinias efektyviai panaudoti analizuodami praktines situacijas.	Paskaitos (probleminis dėstymas), seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas (informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.
Studentai gebės kritiškai vertinti internetinės erdvės tarpvalstybiškumo bei šiuolaikinių informacinių ir komunikacijos technologijų keliamus iššūkius efektyviam teisės aktų taikymui, įrodymų rinkimui, nusikalstamų veikų tyrimui bei bausmių faktiniam įgyvendinimui.	Paskaitos (probleminis dėstymas), seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas (informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.
Studentai gebės aiškiai, taisyklinga teisine kalba nacionaliniu ir tarptautiniu lygmeniu žodžiu ir raštu argumentuotai, kritiškai ir logiškai perteikti įgytas žinias kibernetinio saugumo srityje, pagrįstai dėstyti argumentus, savo idėjas, įžvalgas ir išvadas profesionalų ir neprofesionalų auditorijoms.	Seminarai (minčių lietus, grupės diskusija, situacijų modeliavimas, situacijų simuliacija, atvejo analizė, pristatymai, praktinių užduočių sprendimas), savarankiškas darbas (informacijos paieška, literatūros skaitymas ir analizavimas, procesinių dokumentų rengimas).	Dalyvavimo seminaro metu aktyvumo ir kokybės vertinimas, studentų pristatymų seminarų metu vertinimas, galutinis egzaminas raštu.

Temos	**Kontaktinio darbo valandos**							**Savarankiškų studijų laikas ir užduotys**	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Pagrindiniai informacinių ir komunikacijos technologijų infrastruktūros bei internetinės erdvės subjektai bei jų veikimo principai; kibernetinio saugumo samprata ir pagrindai; grėsmės kibernetiniam saugumui ir jų šaltiniai;	2		2				**4**	**6**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei
2. Kibernetinio saugumo reguliacinė aplinka Lietuvoje ir Europos Sąjungoje; kibernetinio saugumo strategijos formavimas ir ją užtikrinančių subjektų funkcijos nacionaliniu bei ES lygmeniu;	4		2				**6**	**20**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei
3. Privalomosios kibernetinio saugumo rizikos valdymo priemonės finansų bei ypatingos svarbos sektoriuose, jų atitikties nustatytiems reikalavimams vertinimas;	2		2				**4**	**14**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei

4. Produktų gamintojų pareigos kibernetiniam saugumui užtikrinti bei jų nesilaikymo teisinės pasekmės; IT sistemų saugumo sertifikavimas;	2		2				**4**	**14**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei
5. Sistemų pažeidžiamumų samprata, valdymas ir atskleidimas. Verslo subjektų pareigos ir jų nesilaikymo teisinės pasekmės. Verslo subjektų atitikties kibernetinio saugumo reikalavimams užtikrinimas;	2		4				**6**	**22**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei
6. Nusikalstamos veikos kibernetinėje erdvėje; baudžiamasis persekiojimas ir įrodymų rinkimas skaitmeniniame amžiuje; teisėsaugos institucijų tarptautinis bendradarbiavimas; valstybių inicijuotos kibernetinės atakos.	4		4				**8**	**25**	Akademinės literatūros ir teisinių dokumentų skaitymas, internetinio turinio peržiūra ir analizė, pasirengimas diskusijai, prezentacijai ir praktinio atvejo analizei
Iš viso	**16**		**16**				**32**	**101**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Kaupiamasis vertinimas už darbą seminarų metu	10	Semestro metu	1 balas už aktyvumą seminarų metu gali būti skiriamas už rezultatyvų dalyvavimą grupės diskusijose žodžiu: turiningų klausimų ir/ar pastabų teikimas kitiems seminarų dalyviams, jų nuomonės, išvadų, pasiūlymų ir kt. etiškas komentavimas, temos problematikos identifikavimas ir jos suformulavimas, atsakymų į klausimus tikslumas, aiškumas, pagrindimas teisės normomis, moksline literatūra ir teismų praktika. Vertinant dalyvavimą grupės diskusijose, atsižvelgiama ir į tai, ar buvo pasiruošta kiekvienam seminarui, ar buvo studijuojama nurodyta (ir papildoma) medžiaga, ar seminarų dalyvis buvo pats (o ne vien tik dėstytojui kviečiant) iniciatyvus (formalus dalyvavimas seminaruose, t. y. pasyvumas, tylėjimas ar dėstymas tiesiogiai neatsakant į dėstytojo klausimus seminaro tema, skaitymas vadovėlio, konspekto ir pan. gali būti įvertinamas 0 balo). Dalyvavimas seminaruose yra privalomas. Studentui leidžiama laikyti egzaminą be pateisinamos priežasties (liga, artimojo mirtis ir pan.) praleidus ne daugiau nei vieną seminarą. Už didesnę praleistų seminarų dalį privaloma atsiskaityti dėstytojo nustatyta tvarka semestro metu iš anksto susitarus per dėstytojo priėmimo laiką. Atsiskaitymo forma priklauso nuo praleistų seminarų temos ir tuo metu seminaruose vykdytos veiklos. Atvykimas į seminarą nepasiruošus pagal dėstytojo nurodytas užduotis ar medžiagą gali būti prilyginimas seminaro praleidimui be pateisinamos priežasties.
Praktinio atvejo analizės prezentacijos	30	Semestro metu	Seminarų metu studentai privalo parengti ne mažiau nei 3 atvejo analizes ir jas pristatyti pagal dėstytojo suformuluotas užduotis. Kiekviena pristatyta analizė ir jos prezentacija vertinama iki 10 balų. Gauti balai sudedami, padalinami iš pristatytų analizių skaičiaus ir padauginama iš 0.3. Studentui atlikus mažiau nei 3 pristatymus, kaupiamasis balas prilyginamas 0. Atvejo analizė ir jos pristatymas vertinama atsižvelgiant į šiuos kriterijus: - Pristatymo turinys (klausimas išnagrinėtas visapusiškai, kritiškai vertinant problemas bei atlikus išsamią šaltinių analizę); - Pristatymo struktūra (aiškus pristatymo struktūrinių dalių išskyrimas, tikslus sąvokų naudojimas, tinkamas šaltinių citavimas); - Pristatymo stilius (tinkamų vizualinių metodų naudojimas; aiški teisinė kalba; pristatymo įtaigumas ir klausytojų įtraukimas).
Egzaminas	60	Semestro	Egzaminas vykdomas raštu pateikiant studentams 1 praktinio ir 2

		pabaigoje	teorinės analizės pobūdžio atvirojo tipo užduotis. Kiekviena užduotis įvertinama maksimaliai 2 balais. Užduotys formuluojamos siekiant išsiaiškinti studento žinių lygį bei nagrinėtų temų problematikos suvokimą, gebėjimą analizuoti bei remtis moksliniais šaltiniais (vertinamas atsakymų tikslumas, aiškumas ir išsamumas).

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
Sutton, D.	2022	Cyber Security	2nd ed.	BCS, The Chartered Institute for IT
Porcedda, M. G.	2023	Cybersecurity, Privacy and Data Protection in EU Law	1st ed.	Bloomsbury Publishing
Wong, H.	2018	Cyber Security: Law and Guidance	1st ed.	Bloomsbury Professional
Body of European Regulators for Electronic Communication	2022	BEREC Report on the Internet Ecosystem	BoR (22) 167	https://www.berec.europa.eu/system/files/2023-04/20230418_BoR%20%2822%29%20167%20%20BEREC%20Report%20on%20the%20Internet%20Ecosystem.pdf
Spiezia, F.	2022	International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime	Vol. 23	ERA Forum
Eckhardt, P., Kotovskaia A.	2023	The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive	Vol. 4	International Cybersecurity Law Review
Clausmeier, D.	2023	Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)	Vol. 4	International Cybersecurity Law Review
Vandezande, N.	2024	Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor	Vol. 52	Computer Law & Security Review
Papildoma literatūra				
Kittichaisaree, K.	2017	Public International Law of Cyberspace	1st ed.	Springer International Publishing
Wagner. A, Rostow, N.	2020	Cybersecurity and Cyberlaw	1st ed.	Carolina Academic Press
Evans, L.	2020	Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare	1st ed	Bravex Publications
Grabowski, M., Robinson, E.	2021	Cyber Law and Ethics: Regulation of the Connected World	1st ed.	Routledge, Taylor & Francis