STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Internetiniai nusikaltimai	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: doc. dr. Maryja Šupa **Kitas (-i): dokt. Vytautas Kaktinas**	VU Filosofijos fakultetas, Sociologijos katedra, Universiteto g. 9/1, Vilnius

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Individualių studijų dalykas

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	3 semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: –	**Gretutiniai reikalavimai (jei yra): –**

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	144	48	96

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Kurso tikslas – suteikti studentams plačias žinias apie internetinius nusikaltimus, jų techninius, socialinius, teisinius bei ekonominius aspektus. Jos bus papildomos gausia atvejų analize, jų teorinėmis interpretacijomis, technologijų raidos istorija ir diskusijomis apie etines bei kultūrines šiuolaikinių informacijos ir komunikacijos technologijų problemomis. Išklausę kursą studentai gebės vertinti informaciją apie internetinius nusikaltimus, žinos, kokių duomenų reikia norint priimti tinkamus sprendimus šioje srityje, įgys bazines technines žinias bei profesinį žodyną.		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
1.1. Gebės identifikuoti ir suprasti kriminologijos disciplinos sąvokas, apibrėžti bei atpažinti kriminologijos problemas.	Paskaitos, probleminės diskusijos, literatūros analizė, pavyzdžių aptarimas.	Mokymosi refleksija
1.2. Žinos ir supras pagrindines gimineingų kriminologijai dalykų (sociologijos, teisės, psichologijos ir kitų mokslų) koncepcijas ir sąvokas, suvoks kriminologinio žinojimo taikymo sritis.		
3.2. Gebės identifikuoti, analizuoti, nustatyti ir spręsti negatyvių socialinių deviacijų, nusikaltimų kontrolės ir prevencijos, socialines baudžiamosios justicijos problemas, susijusias su konkrečiomis visuomenės struktūromis ir institucijomis, analizuoti šių problemų priežastis ir pasekmes.		
5.2. Gebės savarankiškai plėsti savo žinias ir gebėjimus, vertinti savo profesinius pasiekimus.		
2.1. Gebės savarankiškai suformuluoti kriminologinio tyrimo problemą, argumentuotai pasirinkti ir pagrįsti tam tikrai tyrimo problemai tinkamus tyrimo metodus.	Atvejų pasirinkimas, analizė, teorinis interpretavimas ir pristatymas, diskusijos seminarų metu.	Atvejų analizė

2.2. Gebės savarankiškai ar komandoje, laikantis etinių ir teisinių kriminologinių tyrimų atlikimo reikalavimų, planuoti, organizuoti ir vykdyti kriminologinių tyrimų atlikimą, rinkti duomenis, atlikti šių duomenų analizę ir tinkamai juos interpretuoti.		
3.1. Gebės pasirinkti ir naudotis informaciniais kriminologiniais ištekliais, analizuoti ir sisteminti socialinę ir kriminogeninę informaciją, naudojant šiuolaikines informacines komunikacines technologijas.		
4.1. Gebės raštu ir žodžiu sklandžiai bei aiškiai bendrauti ir pristatyti gautus kriminologinių tyrimų rezultatus profesinėje aplinkoje ir su žmonėmis, kurie nėra profesinės srities ekspertai.		
5.3. Gebės savarankiškai organizuoti ir planuoti savo profesinę veiklą bei priimti sprendimus		

Temos	**Kontaktinio darbo valandos**							**Savarankiškų studijų laikas ir užduotys**	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai	Praktika	**Visas kontaktinis**	**Savarankiškas**	**Užduotys**
1. Internetinių nusikaltimų problematika. Internetinių nusikaltimų samprata ir apibrėžimas. Internetinių nusikaltimų klasifikacija. Socialinis, ekonominis ir teisinis internetinių nusikaltimų kontekstas. Sąsajos su informacijos ir komunikacijos technologijų raida.	2		2				**4**	**2**	Payne, Brian K. 2020. Defining Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 3-26.
2. Internetinių nusikaltimų istorija. Internetinių nusikaltimų sąsaja su telekomunikacijos raida. Žymūs telekomunikaciniai nusikaltimai nuo 19 a. iki dabar. Internetiniai nusikaltimai ir inovacijų ciklas. Internetinių nusikaltimų kaitos veiksniai.	2		2				**4**	**10**	Seminarinė užduotis: žymių internetinių nusikaltimų atlikėjų ir grupuočių analizė.
3. Informacijos ir telekomunikacijos technologijų veikimo principai. Ryšio tinklų komponentai, jų paskirtis ir taikymo galimybės. Duomenų kaupimo ir perdavimo priemonės, debesų kompiuterija, kriptografija.	2						**2**	**2**	Furnell, Steven. Technology Use, Abuse, and Public Perceptions of Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 45-66.
4. Technologijos kaip nusikaltimų objektas 1. Kompiuterių ir kompiuterinių tinklų saugumo spragos ir problematika. Atakų sandara ir žingsniai. Neautorizuota prieiga, DDOS atakos, duomenų manipuliacijos. Nusikaltimams naudojama programinė įranga.	2		2				**4**	**10**	Seminarinė užduotis: Žymių kompiuterinių tinklų saugumo spragų ir atakų analizė.
5. Technologijos kaip nusikaltimų objektas 2. Mobiliojo ryšio infrastruktūros, geolokacijos ir programinės įrangos specifika ir saugumo spragos. Daiktų interneto (Internet of Things), transporto interneto (Internet of Vehicles), mašininės komunikacijos (M2M) specifika, saugumo spragos ir	2						**2**	**10**	Weichbroth, P., Lysik, L. 2020. Mobile Security: Threats and Best Practices, *Mobile Information Systems.*

ateities perspektyvos. Spontaniški tinklai (mesh networking).									Azrour, M., Mabrouki, J., Guezzaz, A., Kanwal, A. 2021. Internet of Things Security: Challenges and Key Issues, *Security and Communication Networks.* Seminarinė užduotis: žymių mobiliųjų tinklų ir daiktų interneto saugumo spragų analizė.
6. Technologijos kaip nusikaltimų objektas 3. Mašininio mokymosi algoritmų veikimo principai iri taikymos sritys. Mašininio mokymosi algoritmų panaudojimas nusikaltimams (adversary AI). Duomenų rinkimo ir analizės automatizavimas neteisėtais būdais.	2		2				**4**	**2**	Caldwell M. et al. 2020. AI-enabled future crime. *Crime Science*, 9.
7. Technologijos kaip nusikaltimų įrankis 1. Technologijų panaudojimas ekonominiams ir finansiniams nusikaltimams: vagystė, sukčiavimas, juodosios rinkos internete. Kriptovaliutų veikimo principai ir saugumo problematika. Ekonominių ir finansinių nusikaltimų kontrolės skaitmeninimas.	2		2				**4**	**10**	Seminarinė užduotis: internetinių finansinių nusikaltimų atvejų analizė.
8. Technologijos kaip nusikaltimų įrankis 2. Intelektinės nuosavybės apsaugos ir viešosios informacijos sklaidos ypatumai ir pažeidimai internete. Informacijos laisvės ir kontrolės problematika internete.	2						**2**	**2**	Jennings, K., Bossler, A. M. 2020. Digital Piracy. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 1025–1046.
9. Technologijos kaip nusikaltimų įrankis 3. Asmens viešumo ir privatumo sampratų ir praktikų kaita. Nepageidaujama rinkodara, sekimas, informacijos nutekinimas, patyčios, neapykantos nusikaltimai. Sintetinių garso ir vaizdo įrašų (deepfake) problematika.	2		2				**4**	**10**	Seminarinė užduotis: informacijos turinio, formos ir platinimo, nusikaltimų prieš asmenis kontraversiškų atvejų analizė.
10. Kriminalistiniai internetinių nusikaltimų tyrimai. Skaitmeninės kriminalistikos šakos, žingsniai, įkalčių rinkimo įrankiai ir metodai. Skaitmeninių įrodymų taikymas teisiniame procese. Skaitmeninė anti-kriminalistika.	2						**2**	**4**	Holt, T. J. 2020. Police and Extralegal Structures to Combat Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 385–402. Rogers, M. 2020. Forensic Evidence and Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 425–446.
11. Internetinių nusikaltimų prevencija. Internetinio saugumo užtikrinimo priemonės pavieniams vartotojams ir organizacijoms. Internetinių saugumo incidentų ir rizikos valdymas. Organizacinė kultūra ir strateginis valdymas kaip internetinių nusikaltimų prevencijos priemonės.	2		2				**4**	**4**	Maimon, D. Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature. In *The Palgrave Handbook of International Cybercrime*

									and Cyberdeviance, p. 449–468. Samtani, S., Abate, M., Benjamin, V., Li, W. 2020. Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 135–154.
12. Teisinis internetinių nusikaltimų reglamentavimas. Informacijos ir telekomunikacijos technologių teisinio reglamentavimo sritys. Tarptautinė ir nacionalinė teisinė aplinka. Jurisdikcijos nustatymo problematika. Baudžiamojo persekiojimo už internetinius nusikaltimus kontraversijos.	2		2				**4**	**2**	da Cruz, J. 2020. The Legislative Framework of the EU Convention on Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 223–238.
13. Tarptautiniai internetinių nusikaltimų aspektai. Tarptautiniai ir organizuoti internetiniai nusikaltimai. Tarptautinės kriminalinės grupės ir jų kultūriniai skirtumai. Haktyvizmas. Informacijos ir telekomunikacijos technologijos kaip nacionalinio saugumo dalis.	2						**2**	**10**	Seminarinė užduotis: skirtingų valstybių kibernetinio saugumo strategijų analizė.
14. Interneto pogrindis ir technologinės subkultūros. Hakerių subkultūros kilmė, raida, filosofija ir etika. Šiuolaikinės technologinės subkultūros.	2						**2**	**4**	Holt, T. J. 2020. Computer Hacking and the Hacker Subculture. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 725–742. Romagna, M. 2020. Hacktivism: Conceptualization, Techniques, and Historical View. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, p. 743–770.
15. Internetiniai nusikaltimai populiariojoje kultūroje. Internetinių nusikaltimų vaizdavimas literatūroje, filmuose, mene. Pagrindiniai žanrai, jų raida ir problematika.	2		2				**4**	**10**	Seminarinė užduotis: internetinių nusikaltimų masinėse medijose ir populiariojoje kultūroje atvejų analizė.
16. Kurso apibendrinimas.	2						**2**	**4**	Kurso pasikartojimas, mokymosi refleksijos pildymas.
Iš viso	**32**		**16**				**48**	**96**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Komandinis darbas – atvejų analizės	80	Seminarų metu	Dirbdami grupėse studentai turi seminarų metu pristatyti 4 temines atvejo analizes pagal iš anksto pateiktą užduotį. Pristatymo trukmė – 15–20 min.

			Kiekvienas pristatymas bus vertinamas 10 balų sistemoje. Vertinimo kriterijai: atvejo analizės išsamumas, pateiktų užduoties klausimų įtraukimas į pristatymą, atsakinėjimas į auditorijos klausimus po pristatymo.
Paskaitų refleksijos	10	Paskaitų metu	Kiekvienos paskaitos pabaigoje studentai turės parašyti trumpą refleksiją, įvertindami įgytas žinias ir kylančius klausimus. Pilnas balas už šį vertinimo aspektą gaunamas, pateikus 10 ir daugiau refleksijų. Pateikus mažiau refleksijų, balas proporcingai mažinamas.
Mokymosi refleksija	10	Semestro pabaigoje	Mokymosi refleksijoje studentai turės apibendrinti savo žinias, įgytas paskaitų ir seminarų metu, aprašyti savarankišką darbą ir indėlį į grupės veiklą, įvertinti stipriąsias ir silpnąsias savo darbo puses. Vertinimo kriterijai: atsakymų išsamumas, kritinis mąstymas.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privaloma literatūra				
Holt, T. J., Bossler, A. M. (eds.)	2020	The Palgrave Handbook of International Cybercrime and Cyberdeviance		https://link.springer.com/referencework/10.1007/978-3-319-78440-3
Weichbroth, P., Lysik, L.	2020	Mobile Security: Threats and Best Practices	Mobile Information Systems, 2020.	https://onlinelibrary.wiley.com/doi/10.1155/2020/8828078
Azrour, M., Mabrouki, J., Guezzaz, A., Kanwal, A.	2021	Internet of Things Security: Challenges and Key Issues	Security and Communication Networks 2021.	https://onlinelibrary.wiley.com/doi/10.1155/2021/5533843
Caldwell M. et al.	2020	AI-enabled future crime	Crime Science, 9	
Papildoma literatūra				
Choucri, Nazli	2012	Cyberpolitics in international relations		Cambridge, Mass.: MIT press
Dhillon, Gurpreet	2014	Essentials of cybersecurity		Washington, DC: Paradigm books
Lewis, James Andrew; Neuneck, Goetz	2013	The cyber index: international security trends and realities		New York: UN
Olson, Parmy	2012	We are Anonymous : inside the hacker world of Lulzsec, Anonymous, and the global cyber insurgency		New York: Little, Brown
Pauli, Josh	2013	The basics of web hacking : tools and techniques to attack the Web		Amsterdam: Syngress
Raymond, Eric S.	2001	The cathedral and the bazaar: musings on Linux and Open source by an accidental revolutionary		Beijing: O'Reilly
Vacca, John R.	2014	Cyber security and IT infrastructure protection		Waltham: Syngress
Sterling, Bruce		Cyberpunk in the nineties		https://w2.eff.org/Misc/Publications/Bruce_Sterling/Interzone_columns/interzone.06
Stephenson, Neal	1996	Mother Earth, Mother Board	Wired, 12.01.96	https://www.wired.com/1996/12/ffglass/
Gibson, William	1995	Neuromancer		London: Harper