STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
SKAITMENINIO TURINIO TEISMINĖ (*FORENSIC*) ANALIZĖ IR KENKSMINGOS PĮ ANALIZĖ	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: Partnerystės docentas Andrius Chaževskas **Kitas (-i):**	Kauno fakultetas Socialinių mokslų ir taikomosios informatikos institutas Muitinės g. 8, LT-44280 Kaunas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	privalomasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	6 semestras	Lietuvių

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Operacinės sistemos ir jų sauga, Informacinės saugos vadyba ir rizikos valdymas	**Gretutiniai reikalavimai (jei yra):** Dirbtinio intelekto (DI) priemonių naudojimas rengiant atsiskaitymo darbus nėra galimas. Atskirais atvejais, tik suderinus su dėstytoju, galimas DI įrankių naudojimas atliekant atskiras praktines skaitmeninės informacijos analizės užduotis. Pavyzdžiui automatinis atvaizdų klasifikavimas (grupavimas), galimų slaptažodžių kandidatų generavimas ir pan.

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	130	52	78

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Ugdyti gebėjimą iš skirtingų skatmeninės informacijos laikmenų nuskaityti, rasti ir ištirti skaitmeninio turinio teisminę informaciją.		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
Gebės taikyti praktikoje teorinius karkasus skaitmeninio turinio informacijai tirti.	Paskaitos, pratybos, savarankiškas darbas aktyvaus mokymo(-si) metodai (grupės diskusija; situacijų analizė), individualieji namų darbai	Laboratoriniai darbai, Individualiųjų namų darbų atsiskaitymas, egzaminas raštu.
Gebės efektyviai kurti ir planuoti skaitmeninė informacijos tyrimo strategijas ir praktiškai surinkti, kvalifikuotai analizuoti ir tirti skaitmeninio turinio informaciją.		
Gebės skaitmeninio turinio teisminės ekspertizės procese taikyti naujausius specializuotus įrankius.		

	Kontaktinio darbo valandos	

Temos	Paskaitos	Konsultacijos	Egzaminas	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. Įvadas į skaitmeninio turinio teisminę ekspertizę (angl. *Digital forensics*). Teismo ekspertų teisės, pareigos ir atsakomybė. Pagrindiniai skaitmeninio turinio informacijos tyrimo žingsniai (identifikacija, nuskaitymas, analizė, pateikimas). Praktiniai pavyzdžiai.	2			2			4	6	Literatūros studijos ([1], 1-2 skyriai).
2. Fizinė duomenų apsauga ir galimos duomenų struktūros laikmenose. Skaidiniai ir failų sistemos (NTFS, FAT). Skaitmeninės informacijos (failų) saugojimo taisyklės ir ištrintos informacijos atstatymo galimybės.	4			4			8	16	Literatūros studijos ([1], 3-6 skyriai); praktinių darbų vykdymas.
3. Skaitmeninio turinio teisminės ekspertizės (angl. *Forensics*) vykdymas taikant atviro kodo programinės įrangos įrankius Linux ir Windows operacinių sistemų pagrindu. Skirtingi failų tipai ir pagrindinių Windows operacinės sistemos skaitmeninių įkalčių (registrų, įvykių žurnalų, nuorodų ir kitų komponentų) peržiūra ir tyrimas. Atviro kodo įrankių (FTK Imager, Autopsy, Event Log Explorer, Log Parser) taikymas.	4			6			10	16	Literatūros studijos ([1], 3-6 skyriai); praktinių darbų vykdymas.
4. Pirmas laboratorinis darbas					2		2		
5. Pagrindiniai atviro kodo programinės įrangos Linux įrankiai skirti vykdyti skaitmeninės informacijos tyrimus. Linux operacinių sistemų sauga, skaitmeninių įkalčių (žurnalų, sisteminių ir vartotojų failų) peržiūra ir tyrimas. Atviro kodo įrankių (FTK Imager, Autopsy ir kitų) taikymas.	2			4			6	10	Literatūros studijos ([1], 7 skyrius); praktinių darbų vykdymas.
6. „Mac“ kompiuterių sauga, operacinių sistemų skaitmeninių įkalčių (žurnalų, sisteminių ir vartotojų failų) peržiūra ir tyrimas. Atviro kodo įrankių (FTK Imager, Autopsy ir kitų įrankių) taikymas.	2			4			6	10	
7. Mobilių įrenginių informacijos sauga, identifikacija, informacijos nuskaitymo galimybės ir metodai, informacijos tyrimas. Duomenų bazių – SQLite failų tyrimas. Atviro kodo įrankių (DB Browser for SQLite, SQLite Studio) praktinis taikymas.	2			4			6	10	Literatūros studijos ([2], 1-2 skyriai); praktinių darbų vykdymas.
8. Antras laboratorinis darbas					2		2		
9. Kompiuterių ir mobiliųjų įrenginių vartotojų slaptažodžių sudėtingumas, slaptažodžių parinkimas naudojant ir saugojimas. Kenksmingos programinės įrangos (PĮ) paieška ir tyrimo galimybės.	2			2			4	10	praktinių darbų vykdymas.
10. Konsultacija		2					2		
11. Egzaminas			2				2		

Iš viso	18	2	2	26	4		52	78	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Individualios namų darbų užduotys (IND)	20	Iki 16 sem. savaitės	Vertinimo kriterijai: atliktų individualių praktinių užduočių skaičius, atliktų užduočių išvadų pagrįstumas, darbo aprašymo kokybė. Kiekvienaa darbas turi vienodą svorį, bendrojo vertinimo.
Laboratorinis darbas Nr. 1 (LD1)	20	8 sav.	Vertinimo kriterijai: atliktų praktinių užsiėmimų metų užduočių skaičius, atliktų užduočių išvadų pagrįstumas, darbo aprašymo kokybė. Kiekvienas darbas turi vienodą svorį, t.y. po 20 % bendrojo vertinimo.
Laboratorinis darbas Nr. 2 (LD2)	20	Iki 16 sem. savaitės	
Egzaminas (E)	40		Egzaminas apima viso dalyko teorinę ir praktinę medžiagą, vertinimas 10 balų skalėje pagal VU vertinimo kriterijus. Egzamino metu pateikiama 20 testo klausimų, į kuriuos egzaminuojamasis turi atsakyti, pasirenkant tinkamą atsakymą. Atsakymai į egzamino klausimus vertinami proporcingai.
Galutinis pažymys: LD1*0,2+LD2*0,2+ IND*0,2+E*0,4=1			

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
1. Bill Nelson, Amelia Phillips, Christopher Steuart	2019	Guide to Computer Forensics and Investigations: Processing Digital Evidence	6t Edition	Cengage Learning, Inc.
2. Christian Hummert Dirk Pawlaszczyk	2022	Mobile Forensics – The File Format Handbook		https://doi.org/10.1007/978-3-030-98467-0
3. JohnSammons	2016	Digital Forensics with the AccessData Forensic Toolkit (FTK)	1st Edition	McGraw-Hill Education; 1 edition (April 5, 2016)
4. Michael K. Robinson	2015	Digital Forensics Workbook: Hands-on Activities in Digital Forensics		CreateSpace Independent Publishing Platform (October 24, 2015)
Papildoma literatūra				
1. The OpenUniversity	2015	Introduction to Computer Forensics andInvestigations		The Open University; 1.0 edition (September 16, 2015)
2. CoryAltheide	2011	Digital Forensics with Open Source Tools	1st Edition	Syngress