STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Skaitmeninių nusikaltimų tyrimai	

Anotacija
Dalykas supažindina su skaitmeninių nusikaltimų tyrimų iššūkiais ir procedūromis. Studentai įgis gebėjimų, kaip reikia taikyti skaitmeninių tyrimų įrankius ir remtis nustatytomis procedūromis, išsaugant duomenis ir užtikrinant proceso atitikimą formaliems dokumentams. Studentai išmoks planuoti tyrimą, rinkti skaitmeninio nusikaltimo įrodymus bei interpretuoti tyrimo rezultatus.

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantis: dr. Agnė Brilingaitė **Kitas (-i):**	Kibernetinio saugumo laboratorija Informatikos institutas Matematikos ir informatikos fakultetas Vilniaus universitetas

Studijų pakopa	Dalyko (modulio) tipas
Antroji	Pasirenkamasis

Įgyvendinimo forma	Vykdymo laikotarpis	Vykdymo kalba (-os)
Auditorinė	Rudens semestras	Anglų

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: IT pradmenys, gebėjimas dirbti komandinėje eilutėje Linux ir Windows OS aplinkoje	**Gretutiniai reikalavimai (jei yra):** -

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	135	48	87

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos
Dalyko tikslas: suteikti studentams kompetencijas, leidžiančias įvykdyti nesudėtingo lygio kibernetinio nusikaltimo tyrimą su apibrėžtomis priemonėmis, įvertinti tyrimo rezultatus ir apie juos komunikuoti, taip

pat gebėti įvardinti nusikaltimo tyrimo etapus ir vertinti sistemų saugumą			
Studijų programos studijų siekiniai	**Dalyko (modulio) studijų siekiniai**	**Studijų metodai**	**Vertinimo metodai**
Rasti, analizuoti ir sisteminti bei vertinti aktualią informaciją, atsirinkti patikimus šaltinius, laikytis etikos principų, pritaikant kitų išvadas, rezultatus.	Remiantis dokumentacija, gerosiomis praktikomis, išskirti nusikaltimų tyrimų procesų gaires, tyrimo rezultatų vertinimo gaires	Literatūros analizė, dokumentacijos sisteminimas ir taikymas, atvejo analizė, refleksija	Projekto gynimas, egzaminas
Prisitaikyti prie realios ar simuliuotos situacijos, identifikuoti esamas problemas, išskirti galimus sprendimus, kūrybiškai ir kokybiškai problemas spręsti, praktiškai taikant turimas žinias.	Tinkamai įvertinti kibernetinio nusikaltimo situaciją, technologinius ir procesinius ribojimus, sudaryti nusikaltimo tyrimo planą	Probleminis dėstymas, praktinės užduotys, eksperimentavimas	Projekto gynimas, egzaminas
Paruošti duomenis analizei, algoritmams bei pateikti duomenis, gautus rezultatus, duomenų ir rezultatų interpretacijas pasinaudojant grafinėmis ar tekstinėmis priemonėmis.	Remiantis procedūromis įvykdyti nusikaltimo tyrimą, nepažeidžiant duomenų, parengti ataskaitą	Praktinės užduotys, eksperimentavimas	Projekto gynimas
Kritiškai analizuoti ir vertinti informacinių sistemų duomenis, procesus ar paslaugas bei informacinių sistemų architektūrose naudojamas technologijas, metodų taikymą.	Tyrimo metu rastus artefaktus susisteminti ir įvertinti	Atvejo analizė, probleminis dėstymas, tęstinės užduotys	Projekto gynimas, egzaminas
Nurodyti grėsmes internete, gebėti pasirinkti tinkamą informacijos saugos būdą, lyginti skirtingus saugos lygmenis.	Identifikuoti galimas grėsmes sistemoms, įvardinti silpnąsias sritis, įvertinti sistemų saugą pagal kontekstinę informaciją	Literatūros analizė, dokumentacijos sisteminimas ir taikymas	Egzaminas

Temos	**Kontaktinio darbo valandos**							**Savarankiškų studijų laikas ir užduotys**	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	Visas kontaktinis darbas	Savarankiškas darbas	**Užduotys**
1.Kibernetinės grėsmės bei skaitmeninių nusikaltimų tyrimai	4			4			**8**	**12**	Grupinis projektas,

									tęstinės praktinės užduotys, atvejo analizė, literatūros (dokumentacijos) analizė
2. Techninė įranga bei OS	2			6			**8**	**15**	
3. Tyrimo tikslas ir jo eiga	3			6			**9**	**15**	
4. Dokumentavimas	2			6			**8**	**15**	
5. Standartai, auditas bei žvalgybinė informacija	3			6			**9**	**15**	
6. Saugumo lygmenys	2			4			**6**	**15**	
Iš viso	**16**			**32**			**48**	**87**	

Vertinimo strategija	Svoris proc.	Atsiskaitymo laikas	Vertinimo kriterijai
Projektas	40	8-12 savaitės	Grupinis darbas, atliekamas dviem etapais, kai pirmas etapas nevertinamas (teikiamas grįžtamasis ryšys). Darbas atliekamas 2-3 studentų grupėje. 50% svorio sudaro techniniai sprendimai,jų dermė ir pagrįstumas problemos sprendimui. 50 % svorio sudaro gynimas – argumentavimas, vertinimo, problematikos komunikavimas.
Egzaminas	60	Sesijos metu (sausio mėn.)	Egzaminą sudaro įvairių tipų klausimų rinkinys, kuriame dauguma klausimų yra atvirieji. Klausimai gali būti tęstiniai, reikalaujantys argumento ar programinio sprendimo fragmento, interpretavimo ir pan.

Autorius	Leidimo metai	Pavadinimas	Periodinio leidinio Nr. ar leidinio tomas	Leidimo vieta ir leidykla ar internetinė nuoroda
Privaloma literatūra				
Hayes, Darren R.	2020	*A Practical Guide to Computer Forensics Investigations*. 2nd edition		Pearson Education
Papildoma literatūra				

COURSE UNIT DESCRIPTION

Course unit title	Code
Digital Forensics	

Annotation
The subject introduces the challenges and procedures of digital forensics. Students will develop skills to apply digital forensics tools and follow the documented procedures to ensure data integrity and compliance to the legislative documents. Students will learn how to plan the investigation, gather digital evidence, and interpret the investigation results.

Lecturer(s)	Department, Faculty
Coordinating: dr. Agnė Brilingaitė **Other:**	Cybersecurity Laboratory Institute of Computer Science Faculty of Mathematics and Informatics Vilnius University

Study cycle	Type of the course unit
Second	Optional

Mode of delivery	Semester or period when it is delivered	Language of instruction
Face-to-face	Autumn	English

Requisites	
Prerequisites: IT basics, skills to use the command line environment in Linux and Windows OS	**Co-requisites (if relevant):**

Number of ECTS credits allocated	Student's workload (total)	Contact hours	Individual work
5	135	48	87

Purpose of the course unit: programme competences to be developed			
The purpose of the study subject is to develop student skills that enable execution of regular digital forensics tasks using defined tooling, evaluation of the results, and communication regarding findings. Also, the subject aims to develop knowledge and skills required to distinguish stages of the forensics processes and assess system security.			
Learning outcomes of the study programme	**Learning outcomes of the course unit**	**Teaching and learning methods**	**Assessment methods**
Ability to search, analyze, process, and evaluate related information, select reliable sources. behave according to ethical principles while applying contributions (results and conclusions) of others.	Distinguish the guidelines for digital forensics processes and evaulation of investigation results using documentation and best practices	Literature review, analysis and application of documentation, case study, and reflection	Project defence, exam
Ability to adapt oneself to the real or simulated situation, identify problems, distinguish possible solutions, solve problems in a creative and qualitative manner by applying knowledge in practice.	Assess the sutuation of the digital crime, techological and process limitations, and prapre the investigation plan	Problem-based learning, practical tasks, experimentation	Project defence, exam
Ability to prepare data for the analysis or for the input of the algorithm, and to present data, results, and data or result interpretations using graphical or text tools/means.	Based on the predifined procesures, execute the digital investigation withou damaging the data and to prepare the report	Practical tasks, experimentation	Project defence
Ability to analyze and evaluate data, processes, or services of information systems and technologies or methods applied in the architectures of information systems.	Organise and evauluate the investigation artefacts	Case study, problem-based learning, continuous tasks	Project defence, exam
Ability to point out internet threats; ability to choose the suitable information security model, and to compare different security levels.	Identify the potential system threats, name weak aspects, and asess the system security based on the contextual information	Literature review, analysis and application of documentation	Exam

Course content: breakdown of the topics	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Workshops	Laboratory work	Internship/work placement	**Contact hours, total**	**Individual work**	**Assignments**
1. Cyber threats and digital forensics	4			4			**8**	**12**	Project, continuous and practical tasks, case studies, literature review
2. Harware and OS	2			6			**8**	**15**	
3. The aim of the investigation and its process	3			6			**9**	**15**	
4. Documentation (reports)	2			6			**8**	**15**	
5. Standards, audit and threat intelligence	3			6			**9**	**15**	
6. Levels of security	2			4			**6**	**15**	
Total	**16**			**32**			**48**	**87**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Project	40	8-12 weeks	The project is implemented as a group work in two stages. During the first stage, the project is not evaluated, as the feedback is provided. The group size is 2-3 students. 50 % of the evaluation is related to technological solutions, their coherence, and argumentation for the problem solution. 50 % of the points are given during the project defence – argumentation, assessment, and overall communication about the problem solved.
Exam	60	Exam session	The exam consists of a set of various questions/tasks, when most of them are open. The questions/tasks can be continuous, requiring reasoning, interpretation, etc.

Author	Publishing year	Title	Issue of a periodical or volume of a publication; pages	Publishing house or internet site
Required reading				

Hayes, Darren R.	2020	A Practical Guide to Computer Forensics Investigations, 2nd edition		Pearson Education
Recommended reading				