STUDIJŲ DALYKO (MODULIO) APRAŠAS

Dalyko (modulio) pavadinimas	Kodas
Kibernetinio saugumo įvadas	

Dėstytojas (-ai)	Padalinys (-iai)
Koordinuojantys: Juozas Dautartas **Kitas (-i):** dr. Arnoldas Budžys	Matematikos ir informatikos fakultetas Duomenų mokslo ir skaitmeninių technologijų institutas

Studijų pakopa	Dalyko (modulio) tipas
Pirmoji	Individualiosios studijos

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

Reikalavimai studijuojančiajam	
Išankstiniai reikalavimai: Studentas turėtų mokėti naudotis Linux/Windows komandine eilute ir suprasti pagrindinius tinklų veikimo principus (IP, DNS, HTTP). Pravartu turėti bet kokios programavimo ar skriptų rašymo patirties (Python, Bash ar pan.), nors tai nėra būtina.	**Gretutiniai reikalavimai (jei yra):**

Dalyko (modulio) apimtis kreditais	Visas studento darbo krūvis	Kontaktinio darbo valandos	Savarankiško darbo valandos
5	134	64	70

Dalyko (modulio) tikslas: studijų programos ugdomos kompetencijos		
Studijų dalyko „Kibernetinio saugumo įvadas“ tikslas – suteikti studentams bendrą supratimą apie kibernetinio saugumo pagrindines sąvokas, gebėjimą identifikuoti dažniausiai pasitaikančių pažeidžiamumų priežastis, suprasti jų pasekmes ir žinoti, kaip jų išvengti. Kursas orientuotas į praktinį saugumo žinių taikymą, todėl studentai mokysis analizuoti informaciją, ieškoti sprendimų ir taikyti prevencines priemones realiose situacijose.		
Dalyko (modulio) studijų siekiniai	**Studijų metodai**	**Vertinimo metodai**
Turės bendrinį supratimą apie kibernetinio saugumo pagrindines sąvokas.	Supratimui – paskaitos, konsultacijos / egzaminas. Gebėjimui taikyti – laboratoriniai darbai, individualus darbas / darbų gynimas. Gebėjimui suprasti literatūrą – individualus darbas, konsultacijos / egzaminas.	Laboratorinių darbų atlikimas bei rezultatų gynimas, egzaminas raštu (atvirojo, pusiau atvirojo bei uždarojo tipo klausimai ir užduotys).
Gebės identifikuoti ir suprasti dažniausiai aptinkamų pažeidžiamumų pasekmes ir priežastis Windows ir Linux sistemose bei jų užkardymą.		
Gebės suvokti kompiuterinio tinklo segmentavimo svarbą bei turės bendrinį suvokimą apie tinklo pažeidžiamumus bei jų užkardymą ar prevenciją.		
Gebės atlikti su kibernetiniu saugumu susijusios informacijos šaltinių paiešką, analizuoti ir praktiškai taikyti juose pateikiamas žinias.		

Temos	Kontaktinio darbo valandos							Savarankiškų studijų laikas ir užduotys	
	Paskaitos	Konsultacijos	Seminarai	Pratybos	Laboratoriniai darbai	Praktika	**Visas kontaktinis darbas**	**Savarankiškas darbas**	**Užduotys**
1. **Įvadas į kibernetinį saugumą.** Įvadas į kibernetinį saugumą – apima informacinio saugumo principus (konfidencialumą, prieinamumą ir vientisumą), pagrindines funkcijas ir atsakomybes šioje srityje, dažniausiai pasitaikančius pažeidžiamumus ir atakų tipus. Taip pat aptariamos grėsmių grupės, jų klasifikacija, taktika, procedūros ir priemonės. Ši tema padeda studentams susiformuoti teorinį pagrindą tolimesniam mokymuisi.	2						2	4	Literatūros analizė, pratybos ir laboratoriniai darbai: praktinis paskaitų turinio taikymas CTF (angl. capture the flag) tipo užduotyse.

2. **Įvadas į tinklo įrangos ir protokolų pažeidžiamumus.** Tinklo įrangos ir protokolų pažeidžiamumai – supažindina su aktyviu ir pasyviu informacijos rinkimu apie kompiuterių tinklus, belaidžių technologijų pažeidžiamumais, tinklo segmentavimo svarba bei tinklo stebėjimo ir apsaugos pagrindais. Studentai mokosi naudotis analizės įrankiais, tokiais kaip Wireshark ar Nmap, ir suprasti, kaip tinklo architektūra gali paveikti saugumą.	12				12		24	20	
3. **Windows ir Linux sistemų atakos vektoriai.** Trečioji tema skirta Windows ir Linux sistemų saugumui. Joje nagrinėjami šių sistemų atakos vektoriai, pažeidžiamumai ir jų prevencija. Studentai susipažįsta su piktavalių naudojamomis taktikomis, ypač atakuojant Windows Active Directory aplinkas, bei mokosi taikyti organizacines saugumo priemones, tokias kaip saugumo stebėsenos sistemos.	12				12		24	20	
4. **Tinklalapių pažeidžiamumai ir atakos vektoriai.** Tinklalapių pažeidžiamumai apima dažniausiai pasitaikančius XSS, SQL įterpimo ir failų įkėlimo pažeidžiamumus. Studentai analizuoja šių pažeidžiamumų veikimo principus ir mokosi juos aptikti bei užkardyti naudodamiesi praktinėmis užduotimis, paremtomis OWASP gairėmis.	6				8		14	16	
5. **Pasiruošimas egzaminui ir egzamino laikymas**.								10	
Iš viso	**32**				**32**		**64**	**70**	

Vertinimo strategija	**Svoris proc.**	**Atsiskaitymo laikas**	**Vertinimo kriterijai**
Pirmasis laboratorinis darbas: tinklo pažeidžiamumų analizė (Nmap, Wireshark).	20	Semestro metu	Studentams skiriami individualūs arba grupiniai darbai, apimantys 1-2 temas. Maksimalus balų skaičius už užduotį yra 20 balų (tai atitinka 20 % viso svorio).
Antrasis laboratorinis darbas: Windows/Linux pažeidžiamumų identifikavimas ir užkardymas.	20	Semestro metu	Studentams skiriami individualūs arba grupiniai darbai, apimantys 2-3 temų turinį. Maksimalus balų skaičius už užduotį yra 20 balų (tai atitinka 20 % viso svorio).
Trečiasis laboratorinis darbas: tinklalapių pažeidžiamumų testavimas naudojant OWASP metodikas.	20	Semestro metu	Studentams skiriami individualūs arba grupiniai darbai, apimantys 3-4 temų turinį. Maksimalus balų skaičius už užduotį yra 20 balų (tai atitinka 20 % viso svorio).
Egzaminas	40	Egzaminų sesijos metu	Studentai gali laikyti baigiamąjį egzaminą, jei yra surinkę minimalų balų skaičių – 30 balų, tai sudaro 50 % bendro laboratorinių darbų įvertinimo. Egzamino metu galima surinkti iki 40 balų, o tai sudaro 40 % galutinio pažymio. Egzamino metu studentai turi parodyti savo žinias apie kurso teorinę dalį (1–4 temos) bei pasiūlyti sprendimą pateiktai problemai. Galimas egzamino laikymas eksternu pateikus išlaikytą HTB Certified Junior Cybersecurity Associate sertifikatą iš HTB Academy.

Autorius	**Leidimo metai**	**Pavadinimas**	**Periodinio leidinio Nr. ar leidinio tomas**	**Leidimo vieta ir leidykla ar internetinė nuoroda**
Privaloma literatūra				
James Forshaw	2024	Windows Security Internals		https://nostarch.com/windows-security-internals Nostarch press, ISBN-13: 9781718501980
OccupyTheWeb	2025	Linux Basics for Hackers, 2nd Edition	2	https://nostarch.com/linux-basics-hackers-2nd-edition Nostarch press, ISBN-13: 9781718503540
Jason Andress	2019	Foundations of Information Security		https://nostarch.com/foundationsinfosec Nostarch press, ISBN-13: 9781718500044
Papildoma literatūra				
HTB Academy	2025	Junior Cybersecurity Analyst Job-Role Path		https://academy.hackthebox.com/preview/certifications/htb-certified-junior-cybersecurity-associate
Malcolm McDonald	2020	Web Security for Developers		https://nostarch.com/websecurity Nostarch press, ISBN-13: 9781593279943

COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Introduction to Cybersecurity	

Lecturer(s)	Department(s) where the course unit (module) is delivered
Coordinator: Juozas Dautartas **Other(s):** Dr. Arnoldas Budžys	Faculty of Mathematics and Informatics Institute of Data Science and Digital Technologies

Study cycle	Type of the course unit (module)
First	Individual studies

Mode of delivery	Period when the course unit (module) is delivered	Language(s) of instruction
face-to-face	Fall semester	Lithuanian

Requirements for students	
Prerequisites: Students are expected to be proficient in using the command line in Linux and Windows and to understand the fundamental principles of how networks work (IP, DNS, HTTP). Experience in programming or scripting (Python, Bash, etc.) is a strong advantage but not required.	**Additional requirements (if any):**

Course (module) volume in credits	Total student's workload	Contact hours	Self-study hours
5	134	64	70

Purpose of the course unit (module): programme competences to be developed		
Aim of the subject (module) is to understand the basic concepts related to cyber security, be able to identify causes of the most common vulnerabilities, understand their consequences, and how to prevent them.		
Learning outcomes of the course unit (module)	**Teaching and learning methods**	**Assessment methods**
Have a common understanding of the basic concepts of cybersecurity.	For understanding - lectures, consultations / exam. To apply the ability - laboratory works, individual work / final work. For the ability to understand literature - individual work, consultations / exam.	Assessment of laboratory assignments, written exam (open, semi-open and closed questions and tasks).
Be able to identify and understand the root causes of most common vulnerabilities in Windows and Linux systems and how to prevent them.		
Will be able to understand the importance of computer network segmentation and will have a general understanding of network vulnerabilities and how to mitigate them.		
Be able to search for resources of information related to cyber security, analyze them, and apply the knowledge presented in them in practice.		

Content: breakdown of the topics	Contact hours							Self-study work: time and assignments	
	Lectures	Tutorials	Seminars	Exercises	Laboratory work	Internship/work placement	**Contact hours**	**Self-study hours**	**Assignments**
1. **Introduction to cybersecurity.** Introduction to cyber security – covers the principles of information security (confidentiality, availability, and integrity), key functions and responsibilities in this area, and the most common vulnerabilities and types of attacks. It also discusses threat groups, their classification, tactics, procedures, and measures. This topic helps students form a theoretical basis for further learning.	2						2	4	Literature analysis, exercises, and laboratory work: practical application of lecture content in CTF (capture the flag) type tasks.

2. **Introduction to network equipment and protocol vulnerabilities.** Network Equipment and Protocol Vulnerabilities – introduces active and passive information gathering on computer networks, wireless technology vulnerabilities, the importance of network segmentation, and the basics of network monitoring and protection. Students learn to use analysis tools such as Wireshark and Nmap and understand how network architecture can affect security.	12				12		24	20	
3. **Attack vectors for Windows and Linux systems.** The third topic is devoted to the security of Windows and Linux systems. It examines the attack vectors and vulnerabilities of these systems and how to prevent them. Students learn about the tactics used by malicious actors, especially when attacking Windows Active Directory environments, and learn how to apply organizational security measures, such as security monitoring systems.	12				12		24	20	
4. **Website vulnerabilities and attack vectors**. Website vulnerabilities include the most common XSS, SQL injection, and file upload vulnerabilities. Students analyze how these vulnerabilities work and learn how to detect and prevent them using practical tasks based on OWASP guidelines.	6				8		14	16	
5. **Preparation for the exam and taking the exam**								10	
Total	**32**				**32**		**64**	**70**	

Assessment strategy	**Weight, %**	**Deadline**	**Assessment criteria**
The first laboratory work: network vulnerability analysis (Nmap, Wireshark).	20	During the semester	Individual or group works are assigned to students covering topics 1-2. The maximum score for the assignment is 20 points (this corresponds to 20% of the total weight).
The second laboratory work: Identification and prevention of Windows/Linux vulnerabilities.	20	During the semester	Individual or group works are assigned to students covering quantum algorithms from topics 2-3. The maximum score for the assignment is 20 points (this corresponds to 20% of the total weight).
The third laboratory work: testing website vulnerabilities using OWASP methodologies.	20	During the semester	Individual or group work is assigned to students covering development and implementation of an algorithm from a case study in topics 3-4. The maximum score for the assignment is 20 points (this corresponds to 20% of the total weight).
Written examination	40	During the exams session	Students can take the final exam if they have earned a minimum of 30 points, which constitutes 50% of the total laboratory work assessment. During the exam, students can earn up to 40 points, which constitutes 40% of the final grade. During the exam, students must demonstrate their knowledge of the theoretical part of the course (topics 1–4) and propose a solution to the problem presented. It is possible to take the exam as an externally by submitting a passed HTB Certified Junior Cybersecurity Associate certificate from HTB Academy.

Author	**Year of publication**	**Title**	**Issue of a periodical or volume of a publication**	**Publishing place and house or web link**
Compulsory reading				
James Forshaw	2024	Windows Security Internals		https://nostarch.com/windows-security-internals Nostarch press, ISBN-13: 9781718501980
OccupyTheWeb	2025	Linux Basics for Hackers, 2nd Edition	2	https://nostarch.com/linux-basics-hackers-2nd-edition Nostarch press, ISBN-13: 9781718503540
Jason Andress	2019	Foundations of Information Security		https://nostarch.com/foundationsinfosec Nostarch press, ISBN-13: 9781718500044
Optional reading				
HTB Academy	2025	Junior Cybersecurity Analyst Job-Role Path		https://academy.hackthebox.com/preview/certifications/htb-certified-junior-cybersecurity-associate
Malcolm McDonald	2020	Web Security for Developers		https://nostarch.com/websecurity Nostarch press, ISBN-13: 9781593279943