COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Cyber Security Technologies	

Lecturer(s)	Department where the course unit is delivered
Coordinator: doc. dr Linas Bukauskas **Other lecturers:**	Department of Computer Science Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
2nd (MA)	Compulsory

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	1st semester	Lithuanian, English

Prerequisites
Prerequisites: General knowledge of information technology, Unix, and basic telecommunications.

Number of credits allocated	Student's workload	Contact hours	Individual work
5	138	64	74

Purpose of the course unit: programme competences to be developed

Generic competences:
-Work and learn independently,
-Think critically and self-critically in the abstract, analyse, organise and evaluate information
-Identify and solve problems.

Specific competences:
- Modelling, designing and specifying IT services/systems after selecting the right infrastructure,
- Apply and evaluate Internet security technologies, their evolution and trends,
- Evaluate information systems architectures,
- Implement, apply and evaluate algorithms relevant to the application task,
- Find and organise specific information from different sources.

Learning outcomes of the course unit:	Teaching and learning methods	Assessment methods
Students will be able to: distinguish the constituent components of the Internet network and understand its operating principles and functions of network protocols.	Inclusive lecture, assignments solution during exercises and independently, studying various sources, submissions preparation and presentation, analysis of situations, data interpretation, design activities, consulting. Practical workshop. Seminars.	Exam test, project defense, tasks decision evaluation, self-assessment tests.
identify, compare, analyze and evaluate Internet security technologies vulnerabilities and threats of cyber-attacks.		
understand the alternatives that ensure the security of networks and information for Internet technologies and choose the optimal one for a specific task or activity.		

Course content: breakdown of the topics	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Practice	Laboratory work	Practical training	**Contact hours**	**Individual work**	**Assignments**
Internet ecosystem and overview of the BGP protocol	2			0			**2**	**2**	Studying literature sources, solving problems
BGP and Internet Connection Protocols TCP/IP, LT Internet infrastructure and IP protocol vulnerabilities	2			4			**6**	**6**	Studying sources, project assignments analysis
TCP, DNS Internet protocol security, Cloud services, Electronic signature, PKI, RSA, ED25519 applications in SSH services	4			4			**8**	**8**	Studying sources, project assignments analysis
Cyber security and "cyber warfare" technologies, national cybersecurity strategies, key concepts	4			4			**8**	**8**	Studying sources, project assignments analysis
Kill chain, intelligence, open source intelligence and perimeter scanning techniques, audio preparation	4			4			**8**	**8**	Studying sources, project assignments analysis, tasks solving
Dark Patterns (workshop) and Social Engineering	8			8			**16**	**16**	Studying sources, project assignments analysis
Risk assessment methodologies for internet services	4			4			**8**	**8**	Studying sources, project assignments analysis
Intrusion monitoring (internal/external) and measures to prevent intrusions	4			4			**8**	**8**	Studying sources, assignments analysis
Preparation for the exam								**10**	Studying sources
Total	**32**			**32**			**64**	**74**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Practical exercises	40	According to the schedule given during the practise	Projects - 100%. Correct theoretical/practical correct solution of a theoretical/theoretical problem, ability to justify the solution; Ability to answer questions related to the algorithm Internet.
Written exam	60	Exam session in January	Written open-ended questions or tasks that require to apply the knowledge acquired. Assessment criteria: - clear presentation of ideas in writing; - the content of the answer is of good quality; - a reasoned solution; - correct solution of a theoretical/practical problem.

Author	Publishing year	Title	Number or volume	Publisher or URL
Required reading				
Chris Hall, Richard Clayton, Ross Anderson,	2011	Inter-X: Resilience of the Internet Interconnection Ecosystem		European Network and Information Security Agency (ENISA)

Evangelos Ouzounis,				
Rytis Rainys	2011	Regionu interneto tinklo infrastrukturos patikimumo tyrimai	ISBN 978-609-457-014-8	VGTU leidykla TECHNIKA
Fernando Gont	2008	Security Assessment of the Internet Protocol		CPNI www.cpni.gov.uk
Joel Weise	2001	Public Key Infrastructure Overview	816-1279-10	Sun Microsystems
William Terrill	2008	WLAN Security Today: Wireless more Secure than Wired		Siemens Enterprise Communications
ENISA	2007	A basic collection of good practices for running a CSIRT	WP2007/2.4.9/1 (CERTD3.1)	ENISA
Recommended reading				
Kari Saarelainen, Heikki Saarinen, Markus Saviaro	2011	Technologies with potential to improve the resilience of the Internet infrastructure	Version 1.0	European Network and Information Security Agency (ENISA)
Tom Olzak	2006	DNS Cache Poisoning: Definition and Prevention		http://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf
Tzeyoung Max Wu	2009	Information Assurance Tools Report – Intrusion Detection Systems	0704-0188	Information Assurance Technology Analysis Center (IATAC)