COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Network Security	**ITSEQ**

Lecturer	Department where the course unit is delivered
Coordinator: lector Martynas Savickas	Department of Computer Science II Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
First	Compulsory

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	6th semester	Lithuanian and English

Prerequisites
Student should have basic knowledge of networking, data transfer methods, understand OSI/TCPIP models, understand networking components.

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
3	75	50	25

Purpose of the course unit: programme competences to be developed

Generic competences to be developed

- Ability to apply knowledge in practical situations *(BK1)*
- Ability for abstract thinking, processing and analysing information *(BK3)*
- Ability to use information and communications technologies *(BK5)*

Subject-specific competences to be developed

- Ability to do program and IT service testing and debugging *(DK4)*
- Ability to evaluate the need of the organization for hardware based on working principles of different computer architectures and various devices *(DK7)*
- Ability to ensure information security using management and security mechanisms of operating systems and software *(DK8)*

Learning outcomes of the course unit	Teaching and learning methods	Assessment methods
Ability to apply secure data transfer methods. Ability to design network models using various units.	Presentation. Case study/analysis.	Evaluation test, exam.
Ability to identify top threats and implement appropriate controls. Ability to analyse attack types and exploitation principles.	Practical exercises using KALI Linux distribution components	Homework and classwork.
Ability to do: object enumeration; vulnerability analysis; analysis of wireless network treats and attack methods. Ability to implement: monitoring model, controls/solution to prevent sniffing and spoofing.	Practical exercises using KALI Linux distribution components	Homework and classwork Evaluation test.

Ability to explain password attack types and principles. Ability to undergo incident and investigation (evidence gathering).		
Ability to manage technical and administrative security controls.	Best practices and security standards analysis and mapping. Compliance management.	Evaluation test. Exam
Ability to make network design and architecture models based on data sensitivity and system functionality.	Presentation. Network architecture and design principals	Homework

Course content: breakdown of the topics	**Individual work: time and assignments**							
	Lectures	Tutorials	Seminars	Laboratory work	Internship/work placement	**Contact hours**	**Individual work**	**Assignments**
1. Secure network architecture	2					**2**	**2**	Literature analysis. Discussion
2. Networking components. Secure data transfer methods.	2			4		**6**		Literature analysis. Classwork
3. Network vulnerabilities. Attack types.	2			24		**26**	**13**	Classwork, tests, homework.
4. Network monitoring	2			4		**6**		Test, homework.
5. Information security framework and governance	2					**2**	**4**	Literature analysis. Discussion. Classwork and homework.
6. Application security. Logical access management.	2					**2**		
7. Secure data management. [Confidentiality, Integrity Availability]	4					**4**	**2**	
Exam preparations		2				**2**	**4**	Exam
Total	**16**	**2**		**32**		**50**	**25**	

Assessment strategy	**Weig ht %**	**Deadline**	**Assessment criteria**
Homework and classwork	30	During semester	During semester student will present three homework reports. Each worth 1 point.
Test/evaluation	40	During semester	Two mid semester tests 2 point each. Each test consists of: one theoretical question worth 0,5 two tasks worth 0,75 point each.
Exam	30	End of semester	Exam evaluation - 3 point. Exam consists of: Two theoretical questions 0,5 point each Two tasks 1 point each

Author	Publishing year	Title	Issue No or volume	Publishing house or Internet site
Required reading				
Shon Harris	2012	CISSP All-in-One Exam Guide. 6th edition		McGraw-Hill
James Broad	2013	Penetration Testing with Kali		Elsevier
Optional reading				
Charlie Kaufman, Radia Perlman, Mike Speciner	2002	Network Security: Private Communication in a Public World. 2nd edition		Prentice Hall
		PCI-DSS V2 security standard	https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0	
		ISO/IEC 27002 security standard. 27002:2009	http://www.lsd.lt/standards/catalog.php?ics=0&pid=634586	