COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
Information Security Fundamentals	

Lecturer(s)	Department(s) where the course unit (module) is delivered
Coordinator: assoc. prof. dr. Igoris Belovas **Other(s):**	Vilnius University Institute of Mathematics and Informatics Akademijos Street 4, LT-08663 Vilnius

Study cycle	Type of the course unit (module)
First	Compulsory

Mode of delivery	Period when the course unit (module) is delivered	Language(s) of instruction
Face-to-face	7th semester	Lithuanian / English

Requirements for students	
Prerequisites: Principles of computer programming, Algorithm theory, Elements of data science	**Additional requirements (if any):** Algebra, Mathematical statistics

Course (module) volume in credits	Total student's workload	Contact hours	Self-study hours
5	133	55	78

Purpose of the course unit (module): programme competences to be developed		
The aim of the course unit is to introduce students to the security issues in information systems, methods designed to protect information systems and practical application of these methods.		
Learning outcomes of the course unit (module)	**Teaching and learning methods**	**Assessment methods**
Ability to solve problems, to organize and schedule work activities with the view to evaluate information security threats and assure organization security politics.	Problem oriented teaching, computer practical exercises, self-study, active learning methods (group discussion, situation analysis)	Self-study, practical group work
Ability to conduct available threats analysis, apply knowledge to security monitoring and systems defend reliability evaluation.	Computer practical exercises, self-study	Self-study, practical group work
Ability to explain the fundamental concepts information security, demonstrate knowledge in cryptography, identification and authentication algorithms application areas.	Problem oriented teaching, computer practical exercises, self-study, active learning methods (group discussion, situation analysis)	Examination, practical assignments
Ability to decide on design organization security solution with the view to secure the sensitive data, consider improvements	Problem oriented teaching, computer practical exercises, self-study	Practical assignments
Ability to select and apply appropriate secure system integration techniques and apply security standards.	Problem oriented teaching, computer practical exercises, self-study, active learning methods (group discussion, situation analysis)	Examination, practical assignments

Content: breakdown of the topics	Contact hours							Self-study work: time and assignments	
	Lectures	Tutorials	Seminars	Exercises	Laboratory work	lacementInternship/work	**Contact hours**	**Self-study hours**	**Assignments**
1. Principles and concepts of information and information system security. Problems, objects and subjects of information security.	2						**2**	**4**	Literature studies.
2. Information security threats. Classifications of cyberattacks and threats. Information security mechanisms.	2						**2**	**4**	Literature studies.
3. Basic concepts in cryptography. Types of cryptosystems. Classical cryptosystems.	2				6		**8**	**10**	Literature studies. Practical tasks.
4. Block ciphers. Basic Concepts in Number Theory and Finite Field. Advanced Encryption Standard. Electronic Code book.	4				7		**11**	**12**	Literature studies. Practical tasks.
5. Pseudorandom Number Generation and Stream Ciphers.	4				6		**10**	**10**	Literature studies. Practical tasks.
6. Asymmetric ciphers. Fermat's and Euler's Theorems. Testing for Primality. The Chinese Remainder Theorem. Public-Key Cryptography and RSA. Digital Signatures.	3				7		**10**	**12**	Literature studies. Practical tasks.
7. Discrete Logarithms. Diffie-Hellman Key Exchange. Elgamal Cryptographic System. Elliptic Curve Arithmetic. Elliptic Curve Cryptography. Cryptographic Hash Functions.	3				7		**10**	**12**	Literature studies. Practical tasks.

8. Organization security instruments. Information system security monitoring and assessment.	2						2	4	Literature studies. Practical tasks.
9. Examination								10	Literature review and preparation for the exam
Total	22				33		55	78	

Assessment strategy	Weight,%	Deadline	Assessment criteria
Laboratory work + Practical work	50 %	At a given time	Laboratory works and their defence; practical exercises performed by the lecturer's instructions in class. Each work is graded. Preparing a summary at the end of the semester workshops report. Assessed in grades 1-10 rating scale: 10-9: Excellent knowledge and skills. Evaluation level. 90-100% of correct answers. 8-7: Good knowledge and skills, there may be minor errors. Synthesis level. 70-89% of correct answers. 6-5: Average knowledge and skills, there are errors. Level of analysis. 50-69% of correct answers. 4-3: Knowledge and skills are below average, the (material) errors. Knowledge application level. 20-49% of correct answers. 2-1: Knowledge and skills do not meet minimum requirements. 0-19% of correct answers.
Examination (E)	50 %	During exam session	The exam consists of questions from the all course material. Assessed in grades 1-10 rating scale: 10-9: Excellent knowledge and skills. Evaluation level. 90-100% of correct answers. 8-7: Good knowledge and skills, there may be minor errors. Synthesis level. 70-89% of correct answers. 6-5: Average knowledge and skills, there are errors. Level of analysis. 50-69% of correct answers. 4-3: Knowledge and skills are below average, the (material) errors. Knowledge application level. 20-49% of correct answers. 2-1: Knowledge and skills do not meet minimum requirements. 0-19% of correct answers.

Author	Year of publication	Title	Issue of a periodical or volume of a publication	Publishing place and house or web link
Compulsory reading				
A. Mikalauskienė, Z. Brazaitis	2010	Informacinių sistemų sauga		Vilnius: Vilniaus universiteto leidykla
G. Skersys	2011	Informacijos sauga		Vilnius: TEV
W. W. Stallings	2017	Cryptography and Network Security: Principles and Practice	6th ed.	Boston, MA: Pearson Education
Optional reading				
E. Kazanavičius [et al.]	2008	Informacijos saugos vadyba		Kaunas: Vitae litera
E. Sakalauskas [et al.]	2008	Elektroninių dokumentų ir duomenų sauga		Kaunas: Vitae litera
E. Sakalauskas [et al.]	2008	Kriptografijos sistemos		Kaunas: Vitae litera
E. Sakalauskas [et al.]	2008	Kriptografijos teorija		Kaunas: Vitae litera
V. Stakėnas	2007	Kodai ir šifrai. Informacijos kodavimo ir kriptografijos pagrindai		Vilnius: Vaistų žinios
R. Šleževičienė	2005	Kriptografijos įvadas		Šiauliai: Šiaulių universiteto leidykla
O. Vasilecas [et al.]	2008	Informacinių sistemų sauga		Vilnius: Technika
A. Venčkauskas, E. Kazanavičius	2011	Informacinių technologijų saugos metodai		Vilnius: TEV
A. Venčkauskas, J. Toldinas	2008	Kompiuterių ir operacinių sistemų sauga		Kaunas: Vitae Litera
S. Azad, A. K. Pathan (eds.)	2019	Practical Cryptography: Algorithms and Implementations using C++		CRC Press/Taylor & Francis Group
M. E. Whitman, H. J. Mattford	2017	Principles of Information Security	6th ed.	Boston, MA : Cengage Learning