COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY	

Academic staff	Core academic unit(s)
Coordinating: assist. dr.Vera Moskaliova	Kaunas Faculty Institute of Language, Literature and Translation Studies ☐ Institute of Social Sciences and Applied Informatics ☒

Study cycle	Type of the course unit
First ☒ Second ☐	Compulsory Course ☒ Optional Couse ☐ Course Unit (Module) of the General University Studies ☐ Course Unit (Module) of Individual Studies ☒ Interdisciplinary Studies Course Unit (Module) ☐

Mode of delivery	Semester or period when it is delivered	Language of instruction
Contact	Autumn semester	English

Requisites	
Prerequisites: *None*	**Co-requisites (if relevant):** *none*

Number of ECTS credits allocated	Student's workload (total)	Contact hours	Individual work
5	130	48	82

Purpose of the course unit		
To develop the ability to analyse, evaluate and apply in practice the security methods of information systems in order to protect these systems from harmful external influences.		
Learning outcomes of the course unit	**Teaching and learning methods**	**Assessment methods**
Will appreciate the importance of IS security and its role in effective management within modern organisations	Lectures, analysis of literature and sources, active learning methods (group discussion; situation analysis)	Active participation in group discussions; completion of practical assignments; exam.
Will be able to identify threats of IS, their causes and possible consequences. Will recognise the IS risk assessment process	Lectures, analysis of literature and sources, active learning methods (group discussion; situation analysis)	Active participation in group discussions; completion of practical assignments; exam.
Will be able to select and apply IS security technologies and methods	Lectures, analysis of literature and sources, active learning methods (group discussion; situation analysis)	Active participation in group discussions; completion of practical assignments; exam.

Content	Contact hours	Individual work: time and assignments

	Lectures	Tutorials	Seminars	Workshops	Laboratory work	Internship	**Contact hours, total**	**Individual work**	**Tasks for individual work**
Understanding of the security of Information and of information systems.	2			2			**4**	**4**	Literature studies ([1], Chapter 1)
Security threats and risks: the causes of the infringements and the offenders. Classification of threats and attacks. Malicious software code	2			4			**6**	**10**	Literature studies: [1], Chapter 3; [2] Chapter 3. Practical tasks: vulnerability scanning, attack modelling.
Cryptography and steganography. Cryptographic systems and algorithms. Electronic signature and its protection. Steganography systems.	2			4			**6**	**10**	Literature studies: [1], Chapter 9. Application of cryptography and cryptanalysis. Practical tasks: Ensuring the confidentiality and integrity of transmitted information through cryptography
Information systems security regulation. Organisational security policies. Security standards. National and international security assessment criteria.	2			4			**6**	**10**	Literature studies: [1], Chapter 12. Practical tasks
Access control and management - Identification and authentication technologies.	2			6			**8**	**14**	Literature studies [1], Chapter 5. Practical tasks
Organisational security measures - Physical security, user training; Incident management	2			4			**6**	**10**	Literature studies [1], Chapter 6. Team work
Ensuring business continuity and efficiency	2			4			**6**	**4**	Literature studies [1], Chapter 8. Practical tasks
Information systems security monitoring and reliability assessment.	2			4			**6**	**6**	Literature studies [1], Chapter 7. Practical tasks
Exam								**14**	Preparation for the exam
Total	**16**			**32**			**48**	**82**	
Note: No more than 4 contact hours may be replaced by guest lectures from social partners or educational visits to social partner organisations									

Assessment strategy	**Weight %**	**Deadline**	**Assessment criteria**
Practical Works (LABs)	20	throughout the semester	The compliance of the completed task with the requirements, the quality of the performance, the student's knowledge and practical skills in the topic of the completed task are assessed. During the semester, up to 10 practical works will take place.

			Assignments are performed from the 1st to the 14th week of the semester. The results of the work will be demonstrated by preparing a Report of practical work, which must be uploaded to emokymai.vu.lt. The Practical work report should be submitted on the due date. In case of delay, the Practical work evaluation is reduced by 1 point per week.
Preparation and presentation of the group work: Academic Research paper (RW)	30	Week 10	Students are assessed on their ability to work in a team, to communicate to achieve a common goal, to plan their time, to independently research, analyse, and review the scientific literature on information systems security, and to present their findings to an audience. The assessment will take into account the content of the academic research work, compliance with the requirements for paper formatting, the quality of the oral presentation, and the answers to the questions.
Quizzes (Qs)	20	throughout the semester	Quizzes consist of 15 questions from each course topic. Quizzes are evaluated on a 10-point scale. During the semester, up to 8 Quizzes will take place.
Exam (E)	30	January, 2027	The exam will take place in a computer classroom, by taking a test on Moodle. The questions are multiple-choice. The student must choose one or more correct answers. The test will consist of 40 questions. The time for solving is 30 minutes. The questions will be given in sequence. There will be no possibility of returning for an earlier question. Evaluation Criteria: **10** - excellent knowledge and skills. 100-91% of correct answers; **9** - very good knowledge and skills, minor mistakes occur; 90-81% of correct answers; **8** - Good knowledge and skills, there are some mistakes; 80-71% of correct answers; **7** - sufficient knowledge and skills, there are mistakes; 70-61% of correct answers; **6** - satisfactory knowledge and skills, there are significant mistakes; 60- 51% of correct answers; **5** - knowledge and skills meet the minimum requirements. There are many mistakes. Level of knowledge and understanding 50-41%; **4-3**: Knowledge and skills are below average, there are (substantial) mistakes. Level of knowledge application. 20-49% correct answers. **2-1**: Minimum requirements not met. 0-19% correct answers.
Final Grade = LABs*0.2+RW*0.3+Qs*0.2+E*0.3, when E >= 5			

REGARDING THE EXTERNAL EXAMINATION OF THE COURSE UNIT

Mark ☒					**If permitted, please provide the conditions**
Not permitted	☒	**Permitted**	☐		

REGARDING THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) TOOLS (SUCH AS "CHATGPT", ETC.) WHEN STUDYING THE COURSE UNIT

Mark ☒				**If permitted, please provide the conditions**
Not permitted	☐	**Permitted**	☒	1. The use of artificial intelligence for course assignments is regulated according to the following document of Vilnius University: *The Guidelines on Artificial Intelligence Usage at Vilnius University*. APPROVED by Resolution No. SPN-54 of 18 June 2024 of the Senate of Vilnius University https://www.vu.lt/site_files/Vertimai/EN_Translation_Dirbtinio_intelekto_naudojimo_Vilniaus_universitete_gair%C4%97s.pdf

				2. The use of AI tools is prohibited during quizzes (Q) and exams (E). Violations of this provision will result in the invalidation of Qs and E grades. 3. If a possible case of inappropriate use of AI is detected during the assessment of theoretical and practical tests, the lecturer may give the student additional test questions to be answered orally. 4. Artificial intelligence tools may be used in the preparation of written work, subject to the following **restrictions**: 4.1 Artificial intelligence tools may be used to create presentation visuals, design elements, and grammatical corrections to the text, provided that this is indicated at the end of the presentation. 4.2 AI tools may **not be used** to generate text content, insights, or conclusions. Cases of use in written work **must be described** in accordance with VU guidelines, i.e., by citing Artificial Intelligence tools in the bibliography as technological tools and indicating how they were used.

REGARDING ACADEMIC PROGRESS
A student who (1) **throughout the semester consistently** fails to demonstrate **progress in achieving the expected learning outcomes of a subject (module)** during the practical classes (seminars, exercises, laboratory work, etc.) and (2) fails to complete all interim assessment requirements and tasks within the time specified in the course description, is not allowed to participate in the examination session.

Author (-s)	Publishing year	Title	Issue of a periodical or volume of a publication	Publishing house or web link
Required reading				
1. Kim D., Solomon M. G.	2018 / 2023	Fundamentals of Information Systems Security	3rd edition / 4th edition	Jones & Bartlett Learning
2. Alan Calder	2020	Cyber Security: Essential Principles to Secure Your Organisation		IT Governance Ltd, https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=6176700
3. Tim Rains	2020	Cybersecurity Threats, Malware Trends, and Strategies : Learn to Mitigate Exploits, Malware, Phishing, and Other Social Engineering Attacks		Packt Publishing Limited, https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=6215711
Recommended reading				
Mark Ciampa	2012	Security + Guide to Network Security Fundamentals	4th edition	Course Technology, Cengage Learning.

NOTE: *Including Open Educational Resources in the reading list is recommended*