



COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
ELECTRONIC PAYMENTS AND THEIR SECURITY	

Academic staff	Core academic unit(s)
Coordinating: Prof. Audrius Lopata Other:	Institute of Social Sciences and Applied Informatics, Kaunas Faculty, Vilnius university

Study cycle	Type of the course unit
First	Mandatory

Mode of delivery	Semester or period when it is delivered	Language of instruction
Face-to-face	4 semester	English

Requisites	
Prerequisites: Fundamentals of Information Systems Security	Co-requisites (if relevant): None

Number of ECTS credits allocated	Student's workload (total)	Contact hours	Individual work
5	133	48	85

Purpose of the course unit		
The aim is to acquaint students with the fundamental knowledge about e-banking technologies and electronic fund transfer systems.		
Learning outcomes of the course unit	Teaching and learning methods	Assessment methods
Students will be able to apply theoretical and practical knowledge necessary for the development of electronic payment solutions	Individual Project, Laboratory classes, Literature analysis	Colloquium (interview conducted by a lecturer and / or specialist), Examination, Individual work, Laboratory examination
Students will be able to put in practice methodologies and tools necessary for electronic payment solution analysis, specification and certification processes.	Individual project, Laboratory classes	Colloquium (interview conducted by a lecturer and / or specialist), Examination, Individual work, Laboratory examination

Content	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Workshops	Laboratory work	Internship	Contact hours, total	Individual work	Tasks for individual work
1. Introduction to e-banking. History, technology types, their advantages and disadvantages, evolution and future trends.	4						4	5	Individual practical assignment
2. Mobile and online banking technology. Hardware and software. Overview of the situation in Lithuania and abroad.	4				4		6	10	Individual practical assignment
3. Architecture of electronic payment solution technologies and their operating principles. Processing principles of electronic payment transactions and the most popular protocols and standards.	8				4		14	20	Individual practical assignment
4. The security of electronic payment systems. The requirements of Payment Card Industry Data Security Standard (PCI DSS). The examples of its practical implementation.	8				4		12	20	Individual practical assignment
5. EMV based hardware and software regulations, specifications and standards, the application for business solutions.	8				4		12	20	Individual practical assignment
6. Preparation for the final examination.								10	
Total	32				16		48	85	

Assessment strategy	Weight %	Deadline	Assessment criteria
Midterm Exam	20	9 th week	Evaluation scale: 10-9: Excellent knowledge and skills. The evaluation level 90-100% correct answers. 8-7: Good knowledge and skills, the answers may contain some minor mistakes. Synthesis level. 70-89% correct answers. 6-5: Average knowledge and skills, the answers containing a number of mistakes. Level of analysis. 50-69% correct answers. 4-3: The level of knowledge and skills is below average, the major errors. The level of knowledge is between 20-49% of correct answers. 2-1: Unsatisfactory results which do not reach the minimum requirements. 0-19% correct answers.
Individual Work and Presentation	20	8-10 week.	Evaluation scale: 10-9: Excellent knowledge and skills. The evaluation level 90-100% correct answers. 8-7: Good knowledge and skills, the answers may contain some minor mistakes. Synthesis level. 70-89% correct answers. 6-5: Average knowledge and skills, the answers containing a number of mistakes. Level of analysis. 50-69% correct answers. 4-3: The level of knowledge and skills is below average, the major errors. The level of knowledge is between 20-49% of correct answers. 2-1: Unsatisfactory results which do not reach the minimum requirements. 0-19% correct answers.
Practical Project	20	13-15 week.	Evaluation scale: 10-9: Excellent knowledge and skills. The evaluation level 90-100% correct answers. 8-7: Good knowledge and skills, the answers may contain some minor mistakes. Synthesis level. 70-89% correct answers. 6-5: Average knowledge and skills, the answers containing a

			number of mistakes. Level of analysis. 50-69% correct answers. 4-3: The level of knowledge and skills is below average, the major errors. The level of knowledge is between 20-49% of correct answers. 2-1: Unsatisfactory results which do not reach the minimum requirements. 0-19% correct answers.
Final examination	40	16th week	Evaluation scale: 10-9: Excellent knowledge and skills. The evaluation level 90-100% correct answers. 8-7: Good knowledge and skills, the answers may contain some minor mistakes. Synthesis level. 70-89% correct answers. 6-5: Average knowledge and skills, the answers containing a number of mistakes. Level of analysis. 50-69% correct answers. 4-3: The level of knowledge and skills is below average, the major errors. The level of knowledge is between 20-49% of correct answers. 2-1: Unsatisfactory results which do not reach the minimum requirements. 0-19% correct answers.

The exam covers the theoretical and practical material of the whole subject, assessment on a 10- point scale according to VU assessment criteria. The final score is calculated according to the formula: Score = Exam * 0.4 + Colloquium * 0.2 + Practical work No.1 * 0.2 + Practical work No.2 * 0.2.

“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				
PCI Security Standards Council	2024	Payment Card Industry Data Security Standard. Requirements and Testing Procedures Version 4.0.1		https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf
PCI Security Standards Council	2025	PCI DSS v4.x Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 4.x		https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4_x-QRG.pdf
PCI Security Standards Council	2025	Payment Page Security and Preventing E-Skimming - Guidance for PCI DSS Requirements 6.4.3 and 11.6.1 Version: 1.0, Revision		https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Guidance-for-PCI-DSS-Requirements-6_4_3-and-11_6_1-r1.pdf
PCI Security Standards Council	2024	Attestation of Compliance for Report on Compliance - Merchants Version 4.0.1		https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Reporting%20Template%20or%20Form/PCI-DSS-v4-0-1-ROC-AOC-Merchants.pdf