VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Reverse Engineering**				
Course code (LAIS):	**MKI_015**				
Study programme:	**CYBERSECURITY ENGINEERING**				
Level of study programme	☐ 1st level professional higher education				
	☐ Professional Bachelor				
	☒ Professional Master				
	☐ PhD level				
Type of Study programme:	☐ Compulsory course (Part A)				
	☒ Professional specialization courses (Part B, compulsory)				
	☐ Professional specialization optional courses (Part B, optional)				
	☐ Elective courses (Part C)				
Course Workload:	**Credits**	**ECTS**	**Academic hours**	**Contact hours**	**Independet work hours**
	1	1.5	40	12	28
Course Author/ Tutor:	**Rūdolfs Gulbis**				
	Academic position		Guest lecturer		
	Consultation: according to the schedule for each semester				
Course Form:	Full time				
Study year, semester	2020/2021	3.sem.			
Language:	Latvian, English				
Prerequisites for the Course:	Knowledges in programming, basic knowledges in Applied Cryptography				
Course summary:	The aim of the study course is to provide in-depth knowledge, to develop an understanding of active, passive, reverse engineering methods to detect, classify software vulnerabilities, create patches and security solutions for information resource protection.				
Course methods:	Lectures, practical classes, seminars, discussions, group work				
The Type of Final examination	Exam				
Requirements for Credits:	Practical work 60%, final exam 40%				
Course content:	Reverse engineering concepts, applications, standards (RFC), operating systems and software knowledge bases, Information resource network testing, functional differences detection and comparison, Code copy acquisition methods, analysis, code comparison				
Learning outcomes	**Learning Outcomes**			**The evaluation methods and criteria**	
	Knowledge				
	The student knows and understands the basic principles of reverse engineering			lectures, practical classes, seminars, discussions, group work	
	Skills				
	The student is able to identify malicious fragments, apply appropriate methods, protection measures			lectures, practical classes, seminars, discussions, group work	
	Competence				
	The student is able to analyze, evaluate malicious code, prepare and provide a testing environment			lectures, practical classes, seminars, discussions, group work	
Course Compulsory literature:	Abhishek Singh, "Identifying Malicious Code Through Reverse Engineering" 2009, ISBN: 0387098240				
Course additional literature:	Kali Linux 2 Assuring Security by Penetration Testing - Third Edition, 2016 Kali Linux Web Penetration Testing Cookbook, 2016 by Gilberto Najera-Gutierrez				
Course approval date:	03.01.2018		**Studiju kursa apraksts aktualizēšanas datums:**		

Study Course plan:

Date*	Theme	Academic hours		Study Form
		Contact lessons	Independent work hours	
	Reverse engineering concepts, applications, standards (RFC), operating systems and software knowledge bases	2		Lecture, discussions, case analysis
	Network testing of information resources (Linux, Win, UNIX) network creation, stress testing, determination and comparison of functional differences	4		Lecture, discussions, case analysis
	Network testing, testing of available service services	2		Lecture, discussions, case analysis
	Code copy retrieval methods, analysis, debugging software, code comparison, virus development tools, detection of their code features.	2		Lecture, discussions, case analysis
	Development of a code test protocol for further analysis, environmental safety and its evaluation		28	Group work, practical work
		2		Final examination
	Hours total:	***12***	***28***	

** The date is specified before the implementation of the course*