VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Data Security and Protection**				
Course code (LAIS):					
Study programme:	**"Information Tehnologies"**				
Level of Study programme:	☒ **1st level professional higher education**				
	☒ **Professional Bachelor**				
	☐ **Professional Master**				
	☐ **Academic 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**	**Independent work hours**
Full time	4	6	160	64	96
Part time	4	6	160	20	140
Course Author/ Tutor:	**Kristaps Felzenbergs**				
	Academical position, scien./acad.degree				
	e-mail: Kristaps.Felzenbergs@va.lv				
	Consultation: according to the schedule for each semester				
Study Form:	Full time studies				
Study year, semester:	2022./2023.				
Language:	English/Latvian				
Prerequisites for the Course:	Ability to express opinion and join discussions				
Course Summary:	The aim of the course is to introduce students with technologies and IT protocols that they use every day possibly even without knowing them. As by understanding the technology in detail that you use can reveal a completely different picture. Within this course students are taken through six essential sections where each of them analyses the security of a given technology which is broadly used. A practical demos and workshops are the key in this course. Key sections of this course include mobile device security, mobile application security and reverse engineering, malware analysis, embedding malware in the application and running that on a testbench or even on a real device in an isolated environment. Also we will look into infrastructure such as mobile networks through generations as GSM/2G and even up to 5G networks, their vulnerabilities and security attributes. WiFi networks is also one of the main topics for this course. When working on this section we setup a local laboratory with appropriate routing equipment and by looking into specific security mechanisms like WEP, WPA and WPA2 analyse their strengths and weaknesses. During the individual work students on their own work on their chosen project which is the main homework during the course. In this phase students work independently to build something using all the knowledge gained from the different subjects and demos experienced in the course previously.				
Assessment:	Lectures, workshops, discussions, work in groups				
Requirements for Credits:	Practical assessments 60%, exam 40%				
Abiding by the Academic Ethics	Students must abide by the academic and research ethics, Vidzeme University of Applied Sciences Ethics Regulations, incl.: – study papers must be independently developed;				

VIDZEMES AUGSTSKOLA

	– the study work should reference all statements, ideas and data used that have been authored by someone else; – appropriate data acquisition methods should be used in the acquisition of data, the research ethics must be respected, empirical data must be collected independently and cannot be distorted or falsified; – the examination must be carried out by the student independently, without the use of supporting materials and/or consultations with other students, unless the lecturer states otherwise. In the event of non-compliance with the academic and research ethics, punishment is imposed in accordance with the ViA Ethics Regulations and the study course must be re-taken, unless the punishment is extramarital.
Learning Outcomes; the evaluation methods and criteria	**Learning Outcomes** / **The evaluation methods and criteria**
	Knowledge
	Broader view on IT solutions and technologies around us / Lectures, workshops, individual work
	Weaknesses and vulnerabilities that can be easily exploited even today / Lectures, workshops, individual work
	Established expertise in Cybersecurity through practical workshops / Lectures, workshops, individual work
	Skills
	Attention to details / Lectures, workshops, individual work
	Competency
	Analyse protocols in various technologies / Lectures, workshops, individual work
	Identify weaknesses in terms of security / Lectures, workshops, individual work
	Evaluate possible mitigation scenarios / Lectures, workshops, individual work
Course Compulsory literature:	Cyber Security Essentials, J.Graham, R.Howard, R.Olson http://index-of.es/Hack/CyberSecuity.pdf
Course additional literature:	
Course confirmation date:	
Date of course description update:	07.11.2022

Study Course Plan for Full Time Students:

Date	Theme	Academic hours		Study Form/ Organization of independent work of students and task description
		Contact hours	Independent work hours	
The date is specified before the implementation of the course	Mobile application source code protection • reverse engineering • embedding a malware • testing behaviour on real devices	**12**	**4**	Lections, workshops
	Mobile device security • data in transit	**8**	**4**	Lections, workshops

	• data at rest • application permissions • information being collected			
	Mobile infrastructure security • GSM/2G/3G/4G/5G networks • Analysis of GSM networks using broadly available tools • Capturing GSM network packets using network packet analysers	**12**	**4**	Lections, workshops
	WiFi network security • WiFi Network security mechanisms WEP, WPA, WPA2 • WiFi radios / antennas (choosing the right equipment for the job) • Hands-on analysis of security mechanisms and their strength with the chosen password complexity (cracking the encryption) • Mand in the middle scenario setup and execution	**16**	**4**	Lections, workshops
	Web application security • Common attack vector analysis • SQL injections • Cross site scripting • Encryption	**8**	**4**	Lections, workshops

	Systems infrastructure security
	• Malware type analysis
	• Building a malware
	  ○ Stealth password collector
	  ○ Crypto worm virus
		8	**4**	Lections, workshops

			62	Security project development
			2	Security project presentation
	Hours total:	***64***	***96***	

Study Course Plan for Part Time Students:

Date	**Theme**	**Academic hours**		**Study Form/ Organization of independent work of students and task description**
		Contact hours	**Independent work hours**	
The date is specified before the implementation of	Mobile application source code protection • reverse engineering	**5**	**16**	Lections, workshops

the course	• embedding a malware testing behaviour on real devices			
	Mobile device security • data in transit • data at rest • application permissions information being collected	**2**	**6**	Lections, workshops
	Mobile infrastructure security • GSM/2G/3G/4G/5G networks • Analysis of GSM networks using broadly available tools Capturing GSM network packets using network packet analysers	**3**	**16**	Lections, workshops
	WiFi network security • WiFi Network security mechanisms WEP, WPA, WPA2 • WiFi radios / antennas (choosing the right equipment for the job) • Hands-on analysis of security mechanisms and their strength with the chosen password complexity (cracking the encryption) Mand in the middle scenario setup and execution	**6**	**24**	Lections, workshops
	Web application security • Common attack vector analysis • SQL injections • Cross site scripting Encryption	**2**	**6**	Lections, workshops
	Systems infrastructure security • Malware type analysis • Building a malware ○ Stealth password collector Crypto worm virus	**2**	**8**	Lections, workshops
			62	Security project development
			2	Security project presentation
	Hours total:	***20***	***140***	