VIDZEMES AUGSTSKOLA

FACULTY OF ENGINEERING
STUDY COURSE DESCRIPTION

Course Title:	**Introduction in Cybersecurity**				
Course code (LAIS):					
Study programme:	**FACULTY OF ENGINEERING**				
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	2	3	80	32	48
Part time	2	3	80	10	70
Course Author/ Tutor:	**Name Surname**				
	Academical position, scien./acad.degree , BA. Andis Maksimovs				
	e-mail: andis.maksimovs@va.lv				
	Consultation: according to the schedule for each semester				
Study Form:	Full time studies/ Part time studies				
Study year, semester:	3rd year, 5th semester				
Language:	English, Latvian				
Prerequisites for the Course:	NIL				
Course Summary:	The goal of this course is to give the students basic understanding of cybersecurity, information security, basic security principles, user awareness and gain an in-depth understing of cyber security risks and their mitigation.				
Assessment:	Theoretical exam, presentation, security assessment and suggestions for a given example company.				
Requirements for Credits:	Active involvement in on-the-spot lectures, discussions. Researched, created and successfully defended cyberattack presentation. Participation and active discussion in CASE studies, and risk assessment example. Participation and successful security assessment creation for given example, with meaningful suggestions. Practical work 70%, final exam 30%				
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; – 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				
	Students know and understand the basic information security principles, user habits and attitudes			lectures, practical classes, seminars, discussions, group work	

VIDZEMES AUGSTSKOLA

	Skills	
	Students are able to find, collect relevant sources of information of cybercrime, counter measures	lectures, practical classes, seminars, discussions, group work
	Competency	
	The student is able to analyse, evaluate information security training samples and make suggestions for their improvement	practical classes, seminars, discussions, group work
Course Compulsory literature:	If available, CSX Cybersecurity Fundamentals, ISACA, 2015	
Course additional literature:	https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf	
Course confirmation date:	30.04.2020	
Date of course description update:	30.04.2020	

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	Introduction into information security, basic security principles, common threats. Malware types, password requirements. Examples, experience	**8**		Lecture, discussions, literature reading.
	A brief questionnaire regarding previous lecture. Security roles in company vs State systems. Security controls, information protection principles, the necessity of risk assessment. Threat and common attack types.	**8**		Lecture, discussions, situational analysis, literature reading.
	Practical assignment: Find and acquire data regarding a successful cyberattack in past 15 years, and create a presentation, explaining when, how, what was taken and how it was dealt with, along with expenses.		8	Individual work
	Student discovered cyberattack presentations and discussions. Security policies, security layers. Cybersecurity controls.	**8**		Individual work result presentations. Lecture, discussions, literature reading.
	Risk assessment example, CASE studies.	**8**		Practical individual work. Discussions. Literature reading.
	Cybersecurity awareness test, DISA.MIL		2	Practical individual work.
	Cybersecurity table top game – “Admins & Networks”.		4	Practical work in teams.

	Assessment of security in company of example, and improvement suggestion writing down and presentation.		24	Practical work in teams.
	Course additional literature reading.		8	Practical individual work.
	Exam – 30 questions.		2	Individual work.
	Hours total:	***32***	***48***	

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 the course	Introduction into information security, basic security principles, common threats. Malware types, password requirements. Examples, experience	**2**	**6**	Lecture, discussions, literature reading.
	A brief questionnaire regarding previous lecture. Security roles in company vs State systems. Security controls, information protection principles, the necessity of risk assessment. Threat and common attack types.		**6**	Lecture, discussions, situational analysis, literature reading.
	Practical assignment: Find and acquire data regarding a successful cyberattack in past 15 years, and create a presentation, explaining when, how, what was taken and how it was dealt with, along with expenses.		8	Individual work
	Student discovered cyberattack presentations and discussions. Security policies, security layers. Cybersecurity controls.	**2**	4	Individual work result presentations. Lecture, discussions, literature reading.
	Risk assessment example, CASE studies.	**3**	4	Practical individual work. Discussions. Literature reading.
	Cybersecurity awareness test, DISA.MIL		2	Practical individual work.
	Cybersecurity table top game – “Admins & Networks”.	3		Practical work in teams.
	Assessment of security in company of example, and improvement suggestion writing down and presentation.		28	Practical work in teams.
	Course additional literature reading.		10	Practical individual work.
	Exam – 30 questions.		2	Individual work.
	Hours total:	***10***	***70***	