RTU Course "Information Systems Security Engineering"

33000 null

General data

Code	DE0753
Course title	Information Systems Security Engineering
Course status in the programme	Compulsory/Courses of Limited Choice; Courses of Free Choice
Responsible instructor	Mārīte Kirikova
Academic staff	Arnis Staško Raimundas Matulevičius
Volume of the course: parts and credits points	1 part, 6.0 credits
Language of instruction	EN
Annotation	The study course introduces students to security risk management. It gives an opportunity to practice security modelling languages and models, analyse security threats and identify security requirements. It includes, also, the topics on security controls (role-based access control, introduction to cryptography), secure software processes, security patterns, and social engineering. The study course was prepared and is consulted by Professor Raimundas Matulevicius, University of Tartu, Estonia.
Goals and objectives of the course in terms of competences and skills	The goal of the study course is to provide students with an overview of the principles of information systems security engineering. The tasks of the study course: 1. To develop student understanding of how to ensure confidentiality, integrity, and availability of secure assets. 2. To develop students understanding of how to engineer and model security requirements and how to use the major security controls, like role-based access control and the principles for the model driven security. 3. To develop student understanding of what are the principles of secure development processes and what the security patterns are.
Structure and tasks of independent studies	Independent studies are integrated with theoretical and practical classes. Every theme has a theory part, a practical part, and independent studies. The independent studies, basically, include assignments where students train and demonstrate their ability to apply theoretical concepts in practice. Individual studies also include preparation for the exam.
Recommended literature	Obligātā/Obligatory: 1. Raimundas Matulevicius. Fundamentals of Secure System Modelling Springer, 2017. Papildu/Additional: 1. Kim, David. Fundamentals of information systems security / David Kim, Michael G. Solomon, xxii, 548 lpp.: ilustrācijas; 24 cm. 2. Whitman, Michael E. Management of information security / Michael E. Whitman, Herbert J. Mattord, xxiv, 728 lpp.: ilustrācijas; 23 cm. 3. Dalpiaz, Fabiano. Security requirements engineering: designing secure socio-technical systems / Fabiano Dalpiaz, Elda Paja, Paolo Giorgini., xxii, 201 lpp.: ilustrācijas; 24 cm.
Course prerequisites	Computer network basics, database basics.

Course contents

Content	Full- and part-time intramural studies		Part time extramural studies	
	Contact Hours	Indep. work	Contact Hours	Indep. work
The conceptual basis of security risk management.	8	12	0	0
Security modeling languages.	10	15	0	0
Security risk and its constituents.	8	12	0	0
Security requirements and their dependencies.	8	12	0	0
Social engineering.	8	12	0	0
Role-based access control and model driven security.	10	15	0	0
Security patterns.	8	12	0	0
Secure software development.	4	6	0	0
Total:	64	96	0	0

Learning outcomes and assessment

Learning outcomes	Assessment methods
Is able, using appropriate technologies, to develop enterprise improvement strategies in the field of information security, to plan analysis and change management projects, and define requirements for new products and services.	Performed practical exercises; exam with theoretical and practical parts.
Is able to identify causes and consequences of (lack of) system and software security.	Performed practical exercises; exam with theoretical and practical parts.

Is able to use the most important techniques to prevent or reduce system and software security problems and to implement and discuss security requirements and security management.	Performed practical exercises; exam with theoretical and practical parts.
Is able to apply advanced modelling techniques (notations, tools, and processes) to build secure systems and software.	Performed practical exercises.
Is able to interpret business concepts of information security in computer science and ICT terms and vice versa.	Performed practical exercises.

Evaluation criteria of study results

Criterion	%
Individual practical exercises	23
Group practical exercises	29
Exam	48
Total:	100

Study subject structure

Part	CP	Hours			Tests			Tests (free choice)		
		Lectures	Practical	Lab.	Test	Exam	Work	Test	Exam	Work
1.	6.0	32.0	32.0	0.0		*			*	