RĪGAS TEHNISKĀ UNIVERSITĀTE

Reģ.Nr.90000068977, Ķīpsalas iela 6A, Rīga, LV-1048, Latvija

Tālr.:67089999; Fakss:67089710, e-pasts:rtu@rtu.lv, www.rtu.lvwww.rtu.lv

Study programme "Cybersecurity Engineering"

Main attributes

Title	Cybersecurity Engineering
Identification code	DMK0
Education classification code	45483
Level and type	Academic Master (Second Cycle) Studies
Higher education study field	Information Technology, Computer Engineering, Electronics, Telecommunications, Computer Control and Computer Science
Head of the study field	Agris Ņikitenko
Deputy head of the study field	Jurģis Poriņš
Department responsible	Faculty of Computer Science, Information Technology and Energy
Head of the study programme	Andrejs Romānovs
Professional classification code	
The type of study programme	Full time
Language	English
Accreditation	29.11.2023 - 30.11.2029; Accreditation certificate No 2023/44-A
Volume (credit points)	120.0
Duration of studies (years)	Full time studies - 2,0
Degree or/and qualification to be obtained	Master degree of engineering science in cybersecurity
Qualification level to be obtained	The 7th level of European Qualifications Framework (EQF) and Latvian Qualifications Framework (LQF)
Programme prerequisites	First cycle higher education in cyber security, information technology, computer science, computer systems, electrical science, or comparable education and an entrance exam. English language skills equivalent to at least B2 level

Description

Abstract	The mission of the academic master’s study programme “Cybersecurity Engineering” is to provide a set of theoretical knowledge and practical skills for students to achieve competencies corresponding to a Master's degree in cybersecurity engineering. In the academic Master's studies, the student acquires the necessary knowledge, skills and competence for comprehensive and effective action in the field of cybersecurity engineering in the chosen economic sector - design, implementation, improvement and management of IT security systems, understanding of professional ethics and socially responsible management, which forms the basis for further studies for a higher level of knowledge and skills acquisition. The role of a cybersecurity specialist in organizations and companies is to manage security solutions, advise users and provide expertise in IT security issues. The implementation of these tasks requires a wide range of knowledge, including security and security management of computer networks, software, integrated systems, and critical infrastructures. RTU Faculty of Computer Science and Information Technology, Faculty of Power and Electrical Engineering and Faculty of Electronics and Telecommunications are the structural units that participate in the implementation of the study programme. Technological and academic support for the program is provided by Palo Alto Networks and Check Point Software Technologies, granting access to their virtual infrastructures, cyberfields, computer networks, training materials, guest lectures, as well as teacher and student certification training on current cybersecurity technologies and approaches.
Aim	The aim of the study programme “Cybersecurity Engineering” is to prepare top level specialists in cybersecurity who can (1) understand and develop the cybersecurity policy of companies and various organizations as well as public space; 2) design, implement, monitor and proactively develop cybersecurity measures; (3) conducting international research in cybersecurity; and (4) continue education for professional development or in doctoral studies.

Tasks	General tasks of the study programme: - to provide competitive academic higher education in accordance with international standards, to prepare students for practical work, to develop skills of scientific research work and to promote their use; - to ensure the development of the content of the study programme, the study process, scientific research work and changes in accordance with the tendencies in the field of cybersecurity, international practice, science and didactic practice; - to provide students with comprehensive knowledge in cybersecurity engineering, to develop specialist skills and competencies in accordance with the requirements of the labour market; - to promote interest in further education and development, supplementation of academic and professional knowledge; - to stimulate students' interest in the processes taking place in society, to stimulate the development of students into a positive, modern, responsible and capable personality who is able to act independently and make decisions independently; - to promote the interaction of the academic staff and students in the performance of scientific research work and in the practical use of the obtained results in accordance with the international standards and tendencies in the field of cybersecurity; - to promote and develop the international exchange and participation of academic staff and students in research projects.
Learning outcomes	As a result of the studies the graduate is able to: - identify, justify and formulate information technology security issues; - design, implement and operate cybersecurity management systems; - analyse, evaluate and develop management systems according to IT security requirements; - develop a corporate digital strategy and align it with the information security strategy; - critically analyse a system monitoring data, identify and manage cybersecurity risks; - apply IT, cybersecurity, data mining and integration tools and techniques, as well as social technologies to protect company information assets; - develop organizational measures and technical solutions for cybersecurity threats; - integrate information security solutions at the network, hardware, software data and process levels and synthesize unified and systemic security management solutions; - ensure safe operation of engineering and socio-technical systems; - provide organizational measures and technical solutions for the protection of the company's critical infrastructure; - assess and ensure that information security solutions meet industry standards and legal requirements; - communicate, advise, collaborate and argue for cybersecurity objectives and outcomes; - independently conduct scientific research in information technologies.
Final/state examination procedure, assessment	At the end of the studies, students must develop a Master thesis in the amount of 30 ECTS. The student develops the master's thesis independently during the last semester of the studies, in consultation with the supervisor. If necessary, the student can arrange consultations with external specialists in the relevant field of research. To successfully complete the study programme students must pass the final state examination which is evaluated according to the 10-point system. Part of the final assessment is the oral defence of the master thesis. The quality of the subject matter, scope, management, literature review, and oral defence are determined by the official "Regulations on the development and defence of the master thesis". The list of possible topics for the Master thesis is confirmed in council meeting by the RTU Institute of Information Technology.
Description of the future employment	Graduates of the study programme are prepared for work in both the state and local government, as well as in the private sector - in commercial companies, small and medium enterprises. The study programme is suitable for students who want to become a cybersecurity analyst, cybersecurity engineer, cybersecurity architect, cybersecurity consultant. Graduates are also prepared for continuing work in industrial research and development as well as in scientific research and higher education.
Special enrollment requirements	Basic requirements: Academic Bachelor degree in engineering or computer sciences, or professional Bachelor degree in the areas of practical activity of the mentioned fields of science, or comparable education. Additional requirements: successful assessment in English in the diploma of previous education, except the case when the previous education was obtained in English.
Opportunity to continue studies	Doctoral studies

Courses

No	Code	Name	Credit points
A		**Compulsory Study Courses**	**60.0**
1	DE0834	Introduction to Cybersecurity	6.0
2	DE0798	Reliability of Information Systems	6.0
3	DE0828	Information Security and Personal Data Protection	6.0
4	DE0831	Cybersecurity Solutions in High Performance Computing Environment	6.0
5	DE0832	Control Fundamentals of Critical Infrastructures	6.0
6	DE0833	Industrial Safety	6.0
7	DE0836	Network Security	12.0
8	DE0829	Software Security	6.0
9	DE0684	Cryptography and Data Security Technologies	6.0
B		**Compulsory Elective Study Courses**	**24.0**
B1		**Field-Specific Study Courses**	**18.0**
1	DE0484	Design of Adaptive Systems	6.0
2	DE0830	Engineering Systems Security	6.0
3	DE0796	Sociotechnical Systems Modelling	6.0
4	DE0642	Data Mining and Knowledge Discovery	6.0
5	DE0778	Project Management	3.0
6	DE0799	Secure E-Commerce Technologies	3.0
7	DE0835	Data integration technologies	3.0
8	DE0738	Enterprise Information Technology Architecture, Applications and Integration	6.0
B2		**Humanities and Social Sciences Study Courses**	**6.0**
1	IV0288	Social Responsibility and Business Ethics	6.0
C		**Free Elective Study Courses**	**6.0**
E		**Final Examination**	**30.0**
1	DE0794	Master Thesis	30.0