**STUDIJŲ DALYKO (MODULIO) APRAŠAS**

| Course unit title | Code |
|---|---|
| FUNDAMENTALS OF SECURITY OF INFORMATION SYSTEMS | |

| Annotation |
|---|
| |

| Lecturer (s) | Department where course unit is delivered |
|---|---|
| **Coordinating: Dr. Vera Moskaliova**<br><br>**Other:** | Kaunas Faculty,<br>Institute of Social Science and Applied Informatics<br>Muitines str. 8, LT-44280 Kaunas |

| Study cycle | Type of the course unit |
|---|---|
| Bachelor | Mandatory, Individual Studies |

| Mode of delivery | Semester or period when it is delivered | Language of instruction |
|---|---|---|
| Class work, Lectures | Autumn Semester | EN |

| Requisites | |
|---|---|
| **Prerequisites: none** | **Co-requisites (if relevant): none** |

| Number of ECTS credits allocated | Student's workload (total) | Contact hours | Individual work |
|---|---|---|---|
| 5 | 130 | 52 | 78 |

| Purpose of the course unit: programme competences to be developed | | |
|---|---|---|
| To develop the ability to analyze, evaluate and apply in practice the security methods of information systems in order to protect these systems from harmful external influences. | | |
| **Learning outcomes of the course unit** | **Teaching and learning methods** | **Assessment methods** |
| Will know the importance of IS security and its management for a modern organization | Lectures, exercises, independent work, active learning methods (group discussion; situation analysis) | Laboratory work |
| Will be able to identify threats of IS, their causes and possible consequences.<br>will know the IS risk assessment process | Lectures, exercises, independent work, active learning methods (group discussion; situation analysis) | Defense of laboratory work. Individual tasks, Research paper. |
| Will be able to select and apply IS security technologies and methods | Lectures, exercises, independent work, active learning methods (group discussion; situation analysis) | Defense of laboratory work. Individual tasks, Exam. |

| Course content: breakdown of the topics | Contact hours | | | | | | | | Individual work: time and assignments |
|---|---|---|---|---|---|---|---|---|---|
| | Lectures | Tutorials | Seminars | Exam | Laboratory work | Internship/work placement | **Contact hours, total** | **Individual work** | **Assignments** |
| Understanding of the security of Information and of Information System. | 2 | | | 2 | | | **4** | **4** | Literature studies ([1], Chapter 1) |
| Security threats and risks: the causes of the infringements and the offenders. Classification of threats and attacks. Malicious software code | 2 | | | 4 | | | **6** | **10** | Literature studies:<br>[1], Chapter 3;<br>[2] Chapter 3.<br>Practical tasks: vulnerability scanning, attack modeling. |
| Cryptography and steganography. Cryptographic systems and algorithms. Electronic signature and its protection. Steganography systems. | 2 | | | 4 | | | **6** | **10** | Literature studies:<br>[1], Chapter 9. Application of cryptography and cryptanalysis.<br>Practical tasks: Ensuring the confidentiality and integrity of transmitted information through cryptography |
| Information systems security regulation. Organizational security policies. Security standards. National and international security assessment criteria. | 2 | | | 4 | | | **6** | **10** | Literature studies:<br>[1], Chapter 12.<br>Practical tasks |
| Access control and management - Identification and authentication technologies. | 2 | | | 6 | | | **8** | **14** | Literature studies<br>[1], Chapter 5.<br>Practical tasks |
| Organizational security measures - Physical security, user training; Incident management | 2 | | | 4 | | | **6** | **10** | Literature studies<br>[1], Chapter 6.<br>Team work |
| Ensuring business continuity and efficiency | 2 | | | 4 | | | **6** | **4** | Literature studies<br>[1], Chapter 8.<br>Practical tasks |
| Information systems security monitoring and reliability assessment. | 2 | | | 4 | | | **6** | **6** | Literature studies<br>[1], Chapter 7.<br>Practical tasks |
| Consultation | | **2** | | | | | **2** | | |
| Exam | | **2** | | | | | **2** | **10** | |
| Iš viso | **16** | **2** | | **32** | | | **52** | **78** | |

| Assessment strategy | Weight % | Deadline | Assessment criteria |
|---|---|---|---|
| Laboratory works | 20 | During senester | The compliance of the completed task with the requirements, the quality of the performance, the student's knowledge and practical skills in the topic of the completed task are assessed. During the semester, 10 laboratory works will take place, the weight of each assessment is 2% of final evaluation.<br>Assignments are performed from the 1st to the 14th week of the semester. The results of the work will be demonstrated by preparing |

| | | | |
|---|---|---|---|
| | | | a Report of laboratory work, which has to be uploaded to the virtual learning environment. The laboratory report should be prepared in two weeks. In case of delay, the evaluation of laboratory work is reduced by 1 point for each week. |
| Preparation and presentation of the individual Research paper | 30 | Week 16 | Students' ability to independently delve, analyze, review and present the results to the audience in their chosen or teacher-appointed information systems security topics is assessed. The evaluation takes into account the content of the work, the design, the quality of the presentation. |
| Project | 20 | Week 8 | The completed project is evaluated on a 10-point scale, taking into account the scope of work, the quality of work, completeness of work, validity of the decision, creativity. |
| Exam | 30 | | The exam is conducted in a virtual learning environment. During the exam, 20 questions are given, to which the examinee must answer in writing, giving theoretical answers, as well as practically illustrating them with examples that correspond to the given question. 1 hour of time is devoted to the exam, during the exam the student can use all the available equipment, as well as can use a computer to search for the necessary information.<br>Evaluation Criteria:<br>**10** - excellent knowledge and skills. 100-91% of correct answers;<br>**9** - very good knowledge and skills, minor mistakes occur; 90-81% of correct answers;<br>**8** - Good knowledge and skills, there are some mistakes; 80-71% of correct answers;<br>**7** - sufficient knowledge and skills, there are mistakes; 70-61% of correct answers;<br>**6** - satisfactory knowledge and skills, there are significant mistakes; 60- 51% of correct answers;<br>**5** - knowledge and skills meet the minimum requirements. There are many mistakes. Level of knowledge and understanding 50-41%;<br>**4-3**: Knowledge and skills are below average, there are (substantial) mistakes. Level of knowledge application. 20-49% correct answers.<br>**2-1**: Minimum requirements not met. 0-19% correct answers. |

| Author | Publishing year | Title | Issue of a periodical or volume of a publication; pages | Publishing house or internet site |
|---|---|---|---|---|
| **Required reading** | | | | |
| 1. Kim D., Solomon M. G. | 2016 | Fundamentals of Information Systems Security | 3rd edition | Jones & Bartlett Learning |
| 2. Alan Calder | 2020 | Cyber Security: Essential Principles to Secure Your Organisation | | IT Governance Ltd, https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=6176700 |
| 3. Tim Rains | 2020 | Cybersecurity Threats, Malware Trends, and Strategies : Learn to Mitigate Exploits, Malware, Phishing, and Other Social Engineering Attacks | | Packt Publishing Limited, https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=6215711 |
| **Recommended reading** | | | | |
| Mark Ciampa | 2012 | Security + Guide to Network Security Funadamentals | 4th edition | Course Technology, Cengage Learning. |