COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Legal Aspects of Cyber Security	

Lecturer (s)	Department where course unit is delivered
Coordinator: Doc. Dr. Paulius Astromskis	Kaunas faculty Institute of Social Sciences and Applied Informatics

Cycle	Level of course unit	Type of the course unit
First	1/1	Mandatory

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Auditorium / Distant	1 Semester	English

Prerequisites and corequisites	
Prerequisites: -	**Corequisites:**

Number of ECTS credits allocated	Student‘s workload	Contact work hours	Individual work hours
5	130	52	78

Purpose of the course unit: programme competences to be developed

To develop the ability to understand, analyze and apply knowledge in the field of cybersecurity and legal regulation

Learning outcomes of course unit	Teaching and learning methods	Assessment methods
Will know and will be able to critically evaluate public and private cyber security laws, information security policies and will be able to independently develop cybersecurity compliance management in the organization Will know and will be able to apply cybercrime evidence and law enforcement in practice, analyze social research or specific legal issues of cyber security Students will acquire: Legal terminology skills of cyber security in solving business problems	Lectures, exercises, individual work Active teaching methods (group discussion, case studies), distance learning forms Research methods: information retrieval, literature analysis, preparation of individual work and presentation	Multiple choice questions exam Assessment of individual work and/or presentations

Course content: breakdown of the topics	Contact work hours							Individual work hours and tasks	
	Lectures	Consultations	Seminars	Practice classes	Laboratory	Practice	**All contact work**	**Individual work**	**Tasks**
1. Introduction to the Cybersecurity Law	2	0,5	1					3	Read: 1) A. Appazov (2014), Legal Aspects of Cybersecurity, pages 9-14; 2) IBM (2022), X-Force Threat Intelligence Index report; 3) IBM (2022), Cost of data breach report; 4) ENISA (2020), Emerging Trends
2. International Cybersecurity Organizations, Policies and Standards	2	0,5	1					3	Read: 1) A. Appazov (2014), Legal Aspects of Cybersecurity, pages 42-67; 2) Cybersecurity Strategy of the European Union; 3) EU Cybersecurity Act; 4) ITU (2021) Guide to Developing a National Cybersecurity Strategy
3. General International Law and Cyberspace	2	0.5	1					3	Read: 1) Tallin Manual 2.0, pages 11 - 78; 168-176 2) Schmitt and Vihul (2016) The Nature of International Law Cyber Norms
4. Specialised Regimes of International Law and Cyberspace	2	0.5	1					3	Read: 1) Tallin Manual 2.0, pages 177-300
5. The Law of Cyber Armed Conflict	2	0.5	1					3	Read: 1) Tallin Manual 2.0, pages 375-511; 2) Valjataga (2022) Cyber vigilantism in support of Ukraine: a legal analysis
6. Substantive Aspects of Cybercrime Law	2	0.5	1					3	Read: 1) A. Appazov (2014), Legal Aspects of Cybersecurity, pages 14-38; 2) Budapest Convention on Cybercrime (Section 1) (and Protocol on Xenophobia and Racism); 3) ENISA (2020) Top 15 Cyber threats
7. Procedural Aspects of Cybercrime	2	0.5	1					3	Read:

Law									1) A. Appazov (2014), Legal Aspects of Cybersecurity, pages 38-42; 2) Budapest Convention on Cybercrime (Section 2) 3) ITU (2014) Understanding cybercrime (pages 238 - 279)
8. General private law and cyberspace	2	0.5	1					3	Read: 1) The EU General Data Protection Regulation (GDPR) 2) Guidelines on Data Protection Impact Assessment (DPIA) 3) EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification; 4) Savin (2016) Jurisdiction Over Cybertorts in the EU – A Coherent Picture?
9. Cybersecurity Risk Management	2	0.5	1					3	Read: 1) Guide to conducting cybersecurity risk assessment for critical information infrastructure (2019); 2) 2018-08-05 Government of the Republic of Lithuania resolution No 818 Description of organisational and technical cyber security requirements imposed on cyber security entities; 3) ENISA (2021) Cybersecurity for SME's
10. Cybersecurity in the public electronic communications sector	2	0.5	1					3	Read: 1) ENISA (2021) Guidelines on security measures under the EECC
11. Cybersecurity in the finance sector	2	0.5	1					3	Read: 1) ENISA (2021) EU Cybersecurity initiatives in the finance sector 2) EBA Guidelines on ICT and security risk management - Štitilis et al (2011) Preconditions for Legal Regulation of Personal Identification in Cyberspace; 3) European Commission (2018) Study on eID and digital on-boarding: mapping and analysis of

									existing on-boarding bank practices across the EU .
12. Cybersecurity in the artificial intelligence sector	2	0.5	1					3	Read: 1) High-Level Expert Group on Artificial Intelligence (2018), ETHICS GUIDELINES FOR TRUSTWORTHY AI 2) EU Artificial Intelligence Act 3) ENISA (2020) AI Cybersecurity Challenges
13. Responsibility for cyber operations	2	0.5	1					3	Read: 1) Hildebrandt (2020), Private Law Liability for Faulty ICT 2) Principles of European Tort Law 3) Tallin Manual 2.0, pages 79-167
14. Cybersecurity Culture	2	0.5	1					3	Read: 1) ENISA (2019) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity
Homework		1						18	
Mid-term exam		1						6	
Exam		1						12	
Iš viso	**28**	**10**	**14**				**52**	**78**	

Assesment strategy	**Comparative weight percentage**	**Date of examination**	**Assesment criteria**
Mid-term exam	20	At the set time	There will be a 15 multiple choice test questions in the MidTerm from the materials prior to MidTerm. It is a closed book exam.
Individual work	30	At the set time	The student will have to perform up to 10 topic related tasks in VU Moodle environment and/or lectures in accordance with the guidelines presented during lectures.
Exam	50	At the set time	There will be a 30 multiple choice test questions in the Final Exam from all materials. It is a closed book exam.
Student knowledge and skills during the examination session are evaluated only when he has fulfilled the requirements and tasks of the intermediate assessment during the semester Students' knowledge and skills during all intermediate evaluations and exam are assessed by grades 1 to 10. The subject matter is calculated if: • the results of all intermediate evaluations are not less than 5; The results of intermediate evaluations are announced in the VU Moodle environment. The final evaluation of the subject is published no later than 4 days after the exam (VU Moodle environment).			

Author	**Year**	**Title**	**Number of periodical publication or publication**	**The place of publication and publisher or online link**

			Volume	
Required reading				
A. Appazov	2014	Legal Aspects of Cybersecurity		Selected readings will be provided through VU Moodle
M. Schmitt	2017	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations		Selected readings will be provided through VU Moodle
M. Schmitt and L. Vihul	2016	The Nature of International Law Cyber Norms		Selected readings will be provided through VU Moodle
A.Valjataga	2022	Cyber vigilantism in support of Ukraine: a legal analysis		Selected readings will be provided through VU Moodle
International Telecommunication Union	2014	Understanding cybercrime		Selected readings will be provided through VU Moodle
A.Savin	2016	Jurisdiction Over Cybertorts in the EU – A Coherent Picture?		Selected readings will be provided through VU Moodle
M. Hildebrandt	2020	Law for Computer Scientists and Other Folk		Selected readings will be provided through VU Moodle
N/A	N/A	Various laws and regulations, including: Cybersecurity Strategy of the European Union; EU Cybersecurity Act; Budapest Convention on Cybercrime; EU General Data Protection Regulation; NIS2 Directive; EU Artificial Intelligence Act; Principles of European Tort Law and other		Selected readings will be provided through VU Moodle
Recommended reading				
A.M. Osula and H. Roigas	2016	International Cyber Norms		
J. Kosseff	2019	Cybersecurity Law		